Exhibit 13

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Gregory G. Raleigh	
U.S. Patent No.:	9,198,117	Attorney Docket No.: 39843-0165IP1
Issue Date:	November 24, 2015	
Appl. Serial No.:	14/667,516	
Filing Date:	March 24, 2015	
Title:	NETWORK SYSTEM WITH COMMON SECURE WIRELESS MESSAGE SERVICE SERVING MULTIPLE APPLICATIONS ON MULTIPLE WIRELESS DEVICES	

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 9,198,117 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

EXHIBITS

SAMSUNG-1001	U.S. Patent No. 9,198,117 to Raleigh ("the '117 Patent")
SAMSUNG-1002	Excerpts from the Prosecution History of the '117 Patent ("the Prosecution History")
SAMSUNG-1003	Declaration and Curriculum Vitae of Dr. Patrick Traynor
SAMSUNG-1004	Complaint, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:23-cv-00103, E.D. Tex., March 10, 2023
SAMSUNG-1005	International Patent Publication. No. WO 2006/077283 A1 ("Houghton")
SAMSUNG-1006	U.S. Patent Publication No. 2007/0011736 Al ("Kalibjian")
SAMSUNG-1007	U.S. Patent Publication No. 2009/0240807 Al ("Munson")
SAMSUNG-1008	U.S. Patent Publication No. 2009/0282256 Al ("Rakic")
SAMSUNG-1009	U.S. Patent Publication No. 2004/0122907 A1 ("Chou")
SAMSUNG-1010	*Security Engineering*, second edition ("Anderson")
SAMSUNG-1011	Declaration of June Munford
SAMSUNG-1012	International Patent Publication. No. WO 2008/048075 A1 ("Lee")
SAMSUNG-1013	U.S. Patent No. 7,082,615 B1 ("Ellison")
SAMSUNG-1014	European Patent No. EP 1 853 044 B1 ("Shenfield")
SAMSUNG-1015	Internet Archive of CryptoGraf, *accessed* Sep. 20, 2023, *available at* https://web.archive.org/web/20070210050616/http://www.cryptograf.com/
SAMSUNG-1016	National Institute of Standards and Technology (NIST) glossary of terms, *accessed* Sep. 20, 2023, *available at* https://csrc.nist.gov/glossary/term/aaa

SAMSUNG-1017	U.S. Patent Publication No. 2004/0105431 A1 ("Monjas-Llorente")
SAMSUNG-1018	U.S. Patent Publication No. 2007/0214245 A1 ("Hämäläinen")
SAMSUNG-1019	Headwater Infringement Contentions, Exhibit B
SAMSUNG-1020	Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings, June 21, 2022, available at *https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf*
SAMSUNG-1021	Docket Control Order, Headwater Research LLC v. Samsung Electronics Co., 2:23-cv-00103-JRG-RSP (EDTX), filed October 27, 2023
SAMSUNG-1022	RESERVED
SAMSUNG-1023	Samsung Stipulation letter regarding IPR grounds in District Court Litigation
SAMSUNG-1024	RESERVED
SAMSUNG-1025	U.S. Patent Publication. No. 2005/0207379 ("Shen")
SAMSUNG-1026	U.S. Patent No. 8,041,816 ("Ozaki")

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1pre]	A network system comprising:
[1.1]	a plurality of device messaging agents, each executable on a respective one of a plurality of mobile end-user devices configured to exchange Internet data via a data connection to a wireless network; and
[1.2]	a network message server supporting a plurality of secure Internet data connections, each secure Internet data connection between the network message server and a respective one of the mobile end-user devices via a device data connection to a wireless network,
[1.3]	the network message server configured to receive, from each of a plurality of network application servers, multiple requests to transmit application data, each such request indicating a corresponding one of the mobile end-user devices and one of a plurality of applications,
[1.4]	the network message server to generate corresponding Internet data messages based on the requests, each such message containing at least one application identifier for an indicated application and application data corresponding to one of the requests, and
[1.5]	the network message server to transmit each of the generated Internet data messages to the device messaging agent located on the device indicated in the corresponding request, using the corresponding secure Internet data connection for the device indicated in the corresponding request;
[1.6]	each device messaging agent, when executing, to receive the Internet data messages from the secure Internet data connection corresponding to the device executing the device messaging agent, and

[1.7]	to, for each received message, map the application identifier in the message to a software process corresponding to the application identifier, and forward the application data in the message to the software process via a secure interprocess communication service.
Claim 2	
[2]	The network system of claim 1, the network message server further to collect and buffer multiple requests to transmit application data to a particular one of the devices.
Claim 3	
[3]	The network system of claim 1, wherein the plurality of applications include a first application that receives the application data in a first format, and a second application that receives the application data in a second format different than the first format.
Claim 4	
[4]	The network system of claim 1, the network message server further to encrypt the secure Internet data messages, the device messaging agents further to decrypt each received message to obtain the corresponding application identifier and application data.
Claim 5	
[5]	The network system of claim 4, wherein the secure Internet data messages are transported to the device messaging agent on each device using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling.
Claim 6	
[6]	The network system of claim 1, wherein the device messaging agent executes in a secure execution environment on at least one of the devices, and at least one of the applications executes outside of the secure execution environment on that device.

Claim 7	
[7.1]	The network system of claim 1, wherein: at least a subset of the device messaging agents, when respectively executing on their respective devices, are each further to receive, from each of multiple applications executing on the corresponding device, at least one corresponding request to transmit application data, each such request indicating a corresponding one of the network application servers,
[7.2]	generate corresponding upload Internet data messages based on the requests, each such message containing at least one server identifier for an indicated application server and application data corresponding to one of the requests, and
[7.3]	transmit each of the generated upload Internet data messages to the network message server, using the corresponding secure Internet data connection for the device; and
[7.4]	the network message server is further to receive the upload Internet data messages over the respective secure Internet data connections, and
[7.5]	for each received upload Internet data message, map the server identifier in that message to a corresponding one of the network application servers, and transmit the application data from that message to the corresponding network application server, together with an indication of the device from which that message was received.
Claim 8	
[8]	The network system of claim 7, wherein at least one of the upload Internet data messages comprises a key for the network application server corresponding to the requesting application.
Claim 9	
[9]	The network system of claim 1, further comprising, on at least one of the devices, the secure interprocess communication service, and

	wherein the secure interprocess communication service and the secure Internet data connection from that device to the network message server are separately secured.
Claim 10	
[10]	The network system of claim 1, wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs.
Claim 11	
[11]	The network system of claim 1, wherein the secure interprocess communication service forwards the application data to at least one of the software processes in an encrypted format.
Claim 12	
[12]	The network system of claim 1, the device messaging agent on at least one of the devices further to initiate the secure connection to the network message server.
Claim 13	
[13]	The network system of claim 1, at least one of the devices having a network stack in communication with the device messaging agent, wherein the secure connection between the network message server and that device is terminated within the network stack.
Claim 14	
[14]	The network system of claim 1, wherein at least one of the applications on at least one of the devices and the network application server corresponding to that application authenticate with each other prior to passing application data via the device messaging agent on that device and the network message server.
Claim 15	

[15]	The network system of claim 1, further comprising a secure server to store a secure authorization list the secure authorization list indicating the applications and network application servers that are allowed to communicate using the network message server.
Claim 16	
[16]	The network system of claim 2, wherein the network message server transmits the collected and buffered requests to the particular device upon the occurrence of a transmission trigger.
Claim 17	
[17]	The network system of claim 16, wherein the transmission trigger is the expiration of a periodic timer.
Claim 18	
[18]	The network system of claim 16, wherein the transmission trigger is the receipt of a transmission from the device messaging agent of the particular device.

Samsung Electronics Co., Ltd. ("**Petitioner**" or "**Samsung**") petitions for *Inter Partes* Review ("**IPR**") of claims 1-18 ("**the Challenged Claims**") of U.S. Patent No. 9,198,117 ("**the '117 Patent**").

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the '117 Patent is available for IPR. This petition is being filed within one year of service of a complaint against Petitioner. Petitioner is not barred or estopped from requesting review of the Challenged Claims on the below-identified grounds.

B. Challenge and Relief Requested

Samsung requests an IPR of the Challenged Claims on the grounds noted below. Dr. Traynor provides supporting testimony in his Declaration. SAMSUNG-1003, ¶¶[1]-[173].

Ground	Claim(s)	35 U.S.C. § 103
1A	1, 3-13	Houghton-Kalibjian
1B	2, 16-18	Houghton-Kalibjian-Munson
1C	14-15	Houghton-Kalibjian-Rakic
2A	1, 3-6, 9-11, 13-15	Lee-Ellison-Anderson
2B	2, 16-18	Lee-Ellison-Anderson-Hämäläinen
3C	7-8, 12	Lee-Ellison-Anderson-Houghton

The '117 Patent claims priority to several provisional applications as early as January 28, 2009 ("Critical Date"). SAMSUNG-1001, Cover. Petitioner does not concede that the claimed priority date is correct, but applies prior art that predates it. The references are prior art under §§102(a), 102(b), and/or 102(e). SAMSUNG-1003, ¶[23].

Reference	Filing Date	Publication Date
Houghton	1/19/2006	7/27/2006
Kalibjian	7/8/2005	1/11/2007
Munson	3/21/2008	9/24/2009
Rakic	5/12/2008	11/12/2009
Anderson	-	2008
Lee	10/19/2007	4/24/2008
Ellison	9/22/2000	7/25/2006
Hämäläinen	3/7/2006	9/13/2007

C. Claim Construction

Petitioner submits that no formal claim constructions are necessary because "claim terms need only be construed to the extent necessary to resolve the controversy." *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir.

2011); SAMSUNG-1003, ¶¶[16]-[19], [23]. Petitioner reserves the right to respond to any constructions offered by Patent Owner or adopted by the Board. Petitioner is not conceding that each challenged claim satisfies all statutory requirements, nor is Petitioner waiving any arguments concerning claim scope or grounds that can only be raised in district court. For this petition, Petitioner applies prior art in a manner consistent with Patent Owner's allegations of infringement before the district court.

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art ("POSITA") relating to the subject matter of the '117 Patent as of January 28, 2009, would have had (1) at least a bachelor's degree in computer science, electrical engineering, or a related field, and (2) 3-5 years of experience in services and application implementation in communication networks. ¶¶21-22. Additional graduate education could substitute for professional experience, and *vice versa*. *Id*.

II. THE '117 PATENT

A. Brief Description

The '117 Patent is directed to "a device messaging agent that securely communicates with a network message server over a wireless network." SAMSUNG-1001, Abstract. The network message server "delivers messages to the device messaging agent on behalf of a plurality of network application servers." *Id*.

These messages include "application data and an indication of a device and an application on the device to which the application data should be delivered." *Id.* The device messaging agent "maps the application identifier to a software process corresponding to the application, and a secure interprocess communication service delivers the application data to that software process." *Id.*; SAMSUNG-1003, ¶[24].

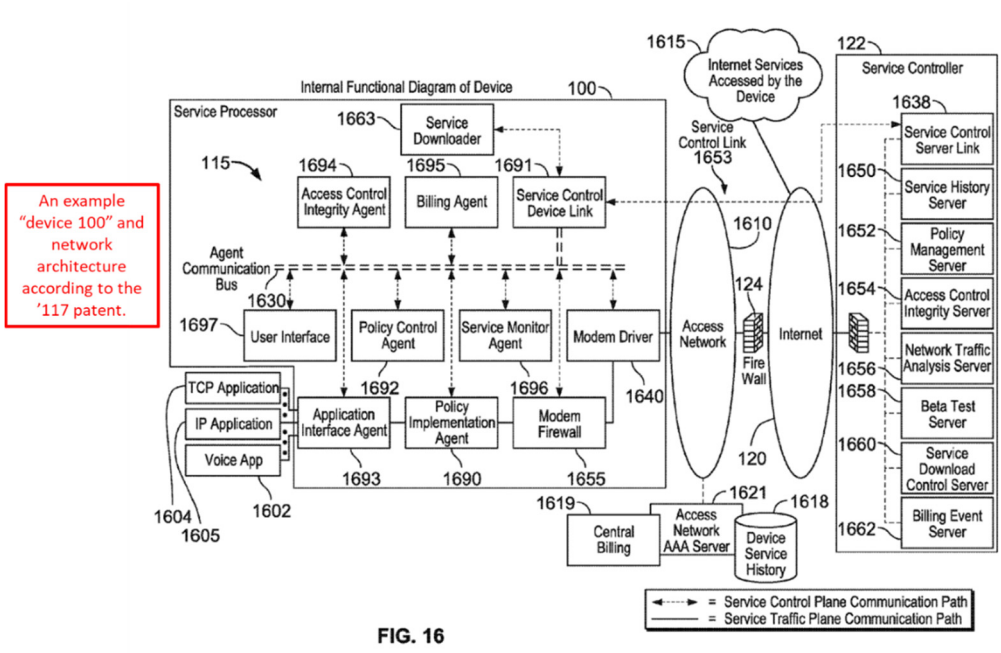


FIG. 16

SAMSUNG-1001, FIG. 16 (annotated). [1]

B. Prosecution History

The '117 Patent was allowed on the first action without any rejections. SAMSUNG-1002, pp. 34-37. During prosecution, the Patent Office did not consider any of the references relied upon in this petition. These references render the Challenged Claims obvious, as discussed below. SAMSUNG-1003, ¶[25].

[1] Annotations to the figures throughout this Petition are shown in color.

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. [GROUND 1A] – Claims 1 and 3-13 are rendered obvious by Houghton and Kalibjian

1. Overview of Houghton[2]

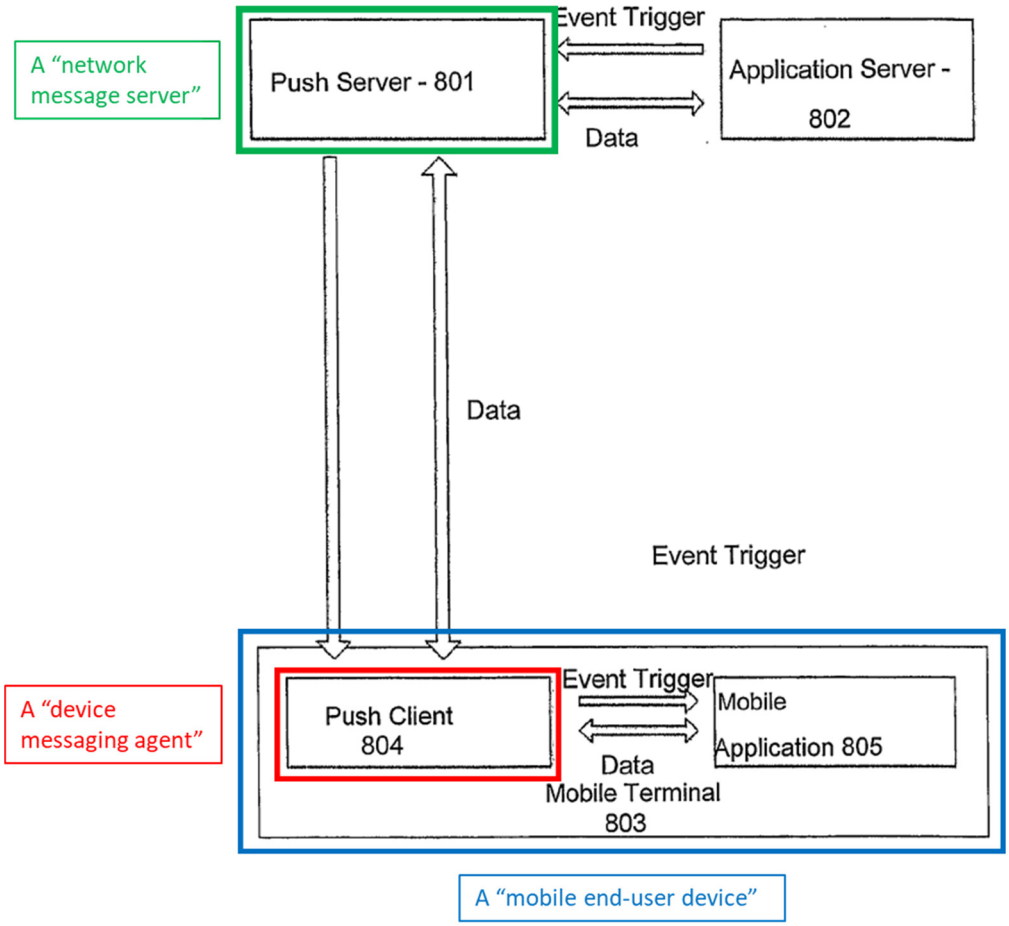
Houghton discloses "[a] server … adapted to push messages to a mobile terminal located in [a] wireless network." SAMSUNG-1005, Abstract. Houghton discloses that these messages "cause programs to start to a specified operating state or, if already started, change [the] operating state to [a] state indicated by the message." *Id*. Houghton discloses a "push client 405 … preferably implemented in the form of a software run in a processor of the mobile terminal 404" and that this mobile terminal is "a portable phone or appliance capable of running software or personal digital assistant." *Id.*, 16:21-25[3]; SAMSUNG-1003, ¶[26].

Houghton also discloses that various secure protocols can be used to implement its push message system. SAMSUNG-1005, 19:14-17 ("HTTPS, IP-Sec, secure IP6 or a proprietary security protocol"). For example, Houghton discloses a "persistent managed, tested and configured data connection … between push

[2] Descriptions of the references and combinations are incorporated into each mapping that includes citations to these references. Emphasis is added to text using bold and/or italicized font unless otherwise indicated.

[3] Citations in Houghton refer to the publication page number.

server 401/801 and push client 405/804." *Id.*, 23:3-21. Houghton additionally discloses "IP or other API (application programming interface) connection[s]" between both the application/push server and client/application exchanges. *Id.*; SAMSUNG-1003, ¶[27].



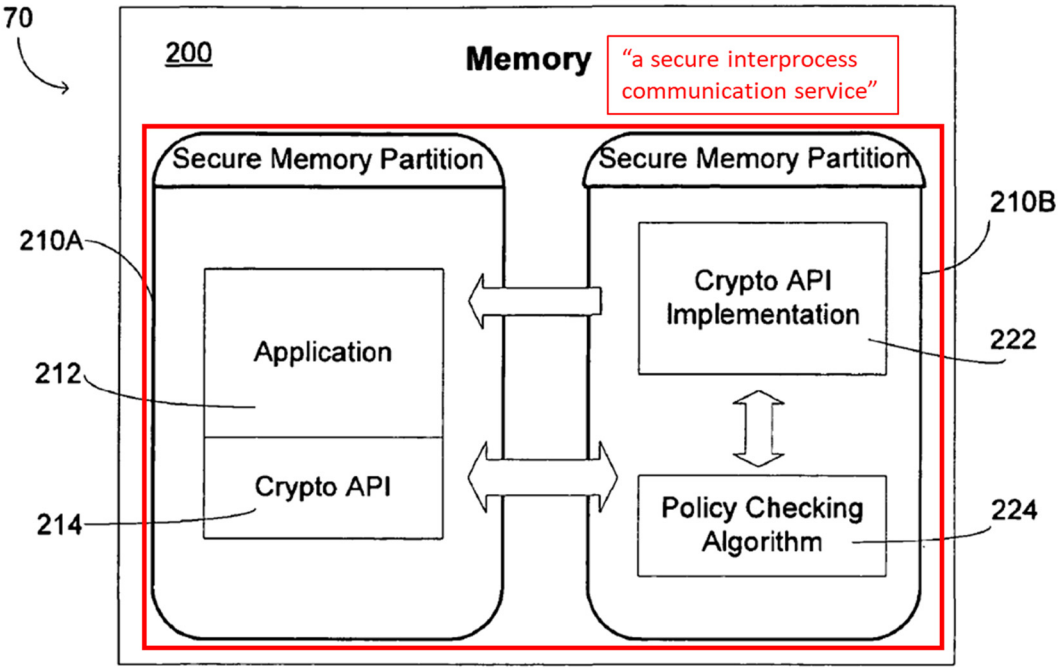
SAMSUNG-1005, FIG. 8 (annotated).

2. Overview of Kalibjian

Kalibjian discloses "policy protected cryptographic Application Programming Interfaces (APIs) that are deployed in secure memory." SAMSUNG-1006, Abstract; ¶¶[0019]-[0021], FIG. 2. Kalibjian's device includes "an application in a

first secure memory partition" that transmits a "request from the application to a cryptographic application programming interface (API)" which is then verified in a "second secure memory partition." *Id.*; SAMSUNG-1003, ¶[28].

The memory of Kalibjian's device is divided into "separate and distinct secure sections" with applications that make "API requests or calls via a secure messaging paradigm." SAMSUNG-1006, ¶¶[0019]-[0021]; *see also* SAMSUNG-1001, 42:45-67, 43:1-4. When applications make requests, a "policy checking algorithm 224 evaluates the request with respect to the established security policy" and permits the communication if it is allowed. SAMSUNG-1006, ¶[0021]. These security policies can include "cryptographic algorithms to use, key sizes, allowable hash algorithms, etc." *Id.*; SAMSUNG-1003, ¶[29].



SAMSUNG-1006, FIG. 2 (annotated).

3. Combination of Houghton and Kalibjian

It would have been obvious to a POSITA to combine the teachings of Houghton and Kalibjian and employ secure interprocess communication in Houghton's devices. SAMSUNG-1003, ¶[30]. As one example, a POSITA would have found it obvious, based on Kalibjian's disclosure, to use secure memory partitions and crypto APIs in the push message system of Houghton. SAMSUNG-1003, ¶[30]; *see supra* §§III.A.1-2. As Dr. Traynor explains, a POSITA would have combined Houghton and Kalibjian to further improve the security of the push message system. SAMSUNG-1003, ¶¶[30]-[33]. For instance:

1) A POSITA would have naturally searched for implementation details for Houghton's API connection between the push client 804 and mobile applications 805. SAMSUNG-1005, 23:3-21. Moreover, a POSITA would have searched for secure APIs because Houghton discloses security as a priority for some customers and gives examples of secure connections and processes. SAMSUNG-1005, 18:28-36, 19:14-17, 19:22-25. This search would have led a POSITA to Kalibjian. SAMSUNG-1006, ¶¶[0019]-[0021], FIG. 2; SAMSUNG-1003, ¶[31].
2) A POSITA would have recognized that crypto APIs, as disclosed in Kalibjian, would have improved the security of Houghton's push message system by improving device security at least because each mobile

terminal acts as an entry point to the network, therefore improving device level security improves network level security by reducing the number of potentially compromised devices using the network. SAMSUNG-1005, 18:28-36, 19:14-17, 19:22-25; SAMSUNG-1006, ¶¶[0019]-[0021], [0025], [0029]-[0030], FIG. 2; SAMSUNG-1003, ¶[32].

3) As Dr. Traynor explains, the increased confidence in device and/or network security provided by Kalibjian would have enabled a POSITA to expand the Houghton push service to additional application servers and clients. SAMSUNG-1005, 18:28-36, 19:14-17, 19:22-25; SAMSUNG-1006, ¶¶[0019]-[0021], [0025], [0029]-[0030], FIG. 2; SAMSUNG-1003, ¶[33].

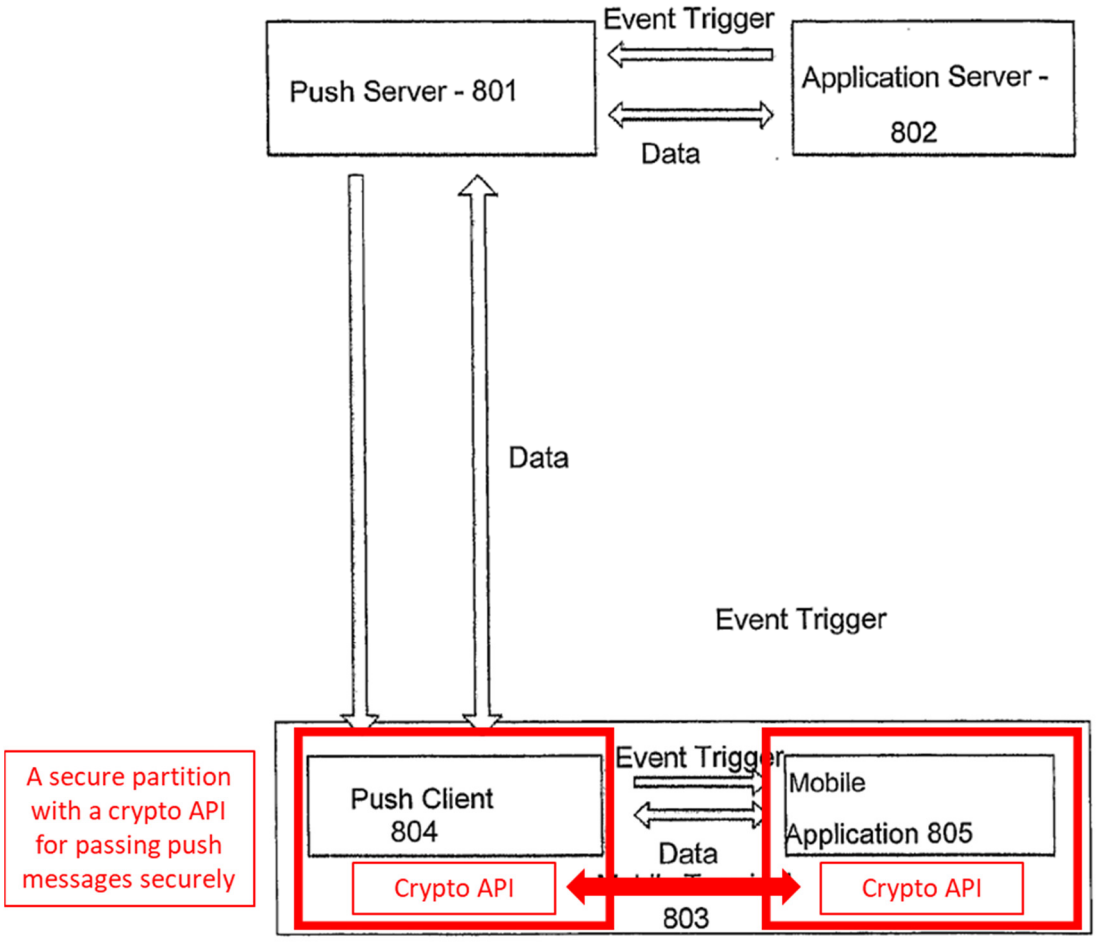
As explained below in more detail, combining Houghton and Kalibjian would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results and (2) the use of known technique to improve similar devices (methods, or products) in the same way. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007)*;* MPEP §2143; SAMSUNG-1003, ¶[34].

Incorporating secure memory partitions and crypto APIs into Houghton's push message system would also have been predictable and foreseeable with a reasonable expectation of success at least because Houghton discloses the use of APIs

for communicating between program modules. SAMSUNG-1005, 23:3-21; SAMSUNG-1003, ¶[35]. Additionally, Kalibjian discloses that its techniques can be implemented as "software," which would have been well within the capability of a POSITA to implement in Houghton's mobile terminals. SAMSUNG-1006, ¶¶[0031], [0046]. Moreover, Houghton discloses security protocols, such as "HTTPS, IP-Sec, secure IP6 or a proprietary security protocol to identify the communicating parties, prevent message interception by 3rd parties, and prevent message modification by 3rd parties," thus illustrating that security was a concern in the Houghton system. SAMSUNG-1005, 19:14-17, 23:3-28. Kalibjian also discloses that its techniques "can employ various protocol known to those skilled in the art, such as the Transmission Control Protocol/Internet Protocol ('TCP/IP') over a number of alternative connection media, such as cellular phone, radio frequency networks, satellite networks, etc. or UDP (User Datagram Protocol) over IP." SAMSUNG-1006, ¶[0016]. Additionally, Kalibjian discloses that its methods can be implemented in "cellular communication devices (such as cellular telephones)" consistent with the mobile terminals Houghton describes. SAMSUNG-1005, 16:16-36, 17:1-2; SAMSUNG-1006, ¶[0011]; SAMSUNG-1003, ¶[35].

In one example of the combined Houghton-Kalibjian system, illustrated below in modified Figure 8 from Houghton, Kalibjian's secure memory partitions and crypto APIs would have been incorporated into Houghton's mobile terminal

such that they would provide additional security when passing messages between the push client and mobile applications. SAMSUNG-1005, 18:28-36, 19:14-17, 19:22-25, 23:3-21; SAMSUNG-1006, ¶¶[0019]-[0021], FIG. 2; SAMSUNG-1003, ¶[36]. In the combined system, the push client would operate within a secure partition and send push messages to other secure partitions containing device applications with a crypto API. SAMSUNG-1005, 18:28-36, 19:14-17, 19:22-25, 23:3-21; SAMSUNG-1006, ¶¶[0019]-[0021], FIG. 2; SAMSUNG-1003, ¶[36].



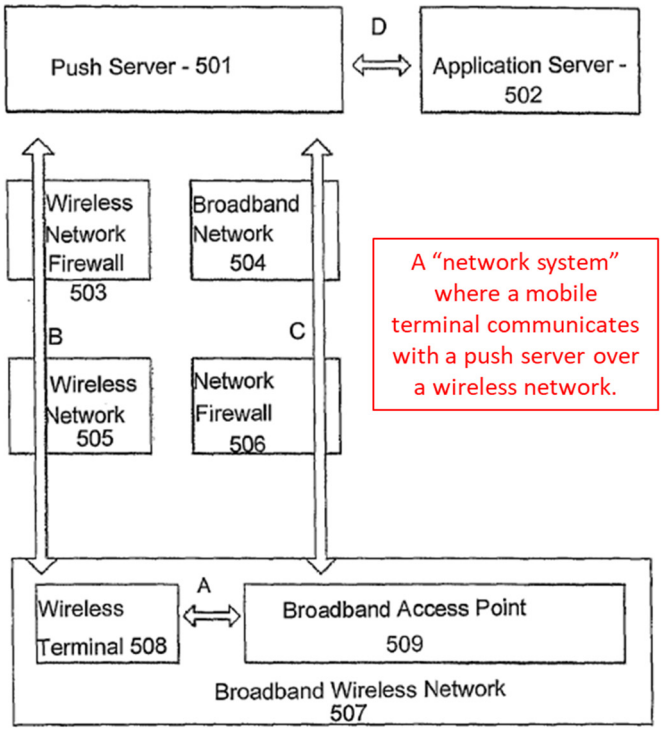
SAMSUNG-1005, FIG. 8 (modified to incorporate Kalibjian).

4. Analysis

[1.pre]

To the extent the preamble is limiting, Houghton renders it obvious. Specifically, Houghton discloses a server "adapted to push messages to a mobile terminal" located in a "wireless network" ("***a network system***"). SAMSUNG-1005, Abstract, 11:5-36, 16:16-36, 17:1-2, 19:1-36, 20:1-28, FIGS. 1-5, 7-9. As one example, Houghton's Figure 5 illustrates a mobile terminal 503 in communication with a push server 501 over a wireless network 505. SAMSUNG-1005, FIG. 8; SAMSUNG-1003, ¶[37].

Figure 5



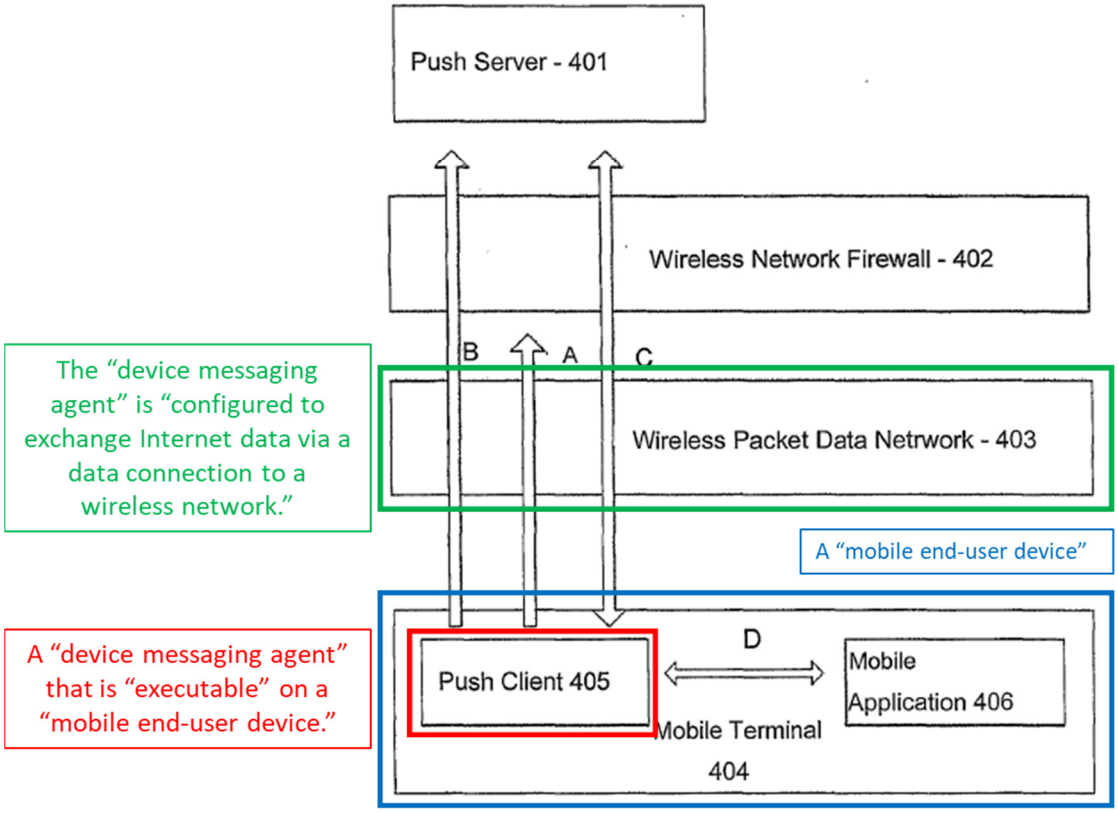
SAMSUNG-1005, FIG. 5 (annotated).

[1.1]

Houghton discloses a "push client 405[4]" ("***device messaging agent***") that is "implemented in the form of a software run in a processor of the mobile terminal 404" and "launches automatically when the mobile terminal 404 is turned on" ("***executable on a respective one of a plurality of mobile end-user devices***"). SAMSUNG-1005, 16:16-26, 17:3-12, FIGS. 4, 7-9. Houghton also discloses that push clients 405 communicate with a "push server 401 over a data network 403, normally a wireless network capable of transmitting Internet Protocol (IP) packets" ("***devices configured to exchange Internet data via a data connection to a wireless network***"). SAMSUNG-1005, 16:16-20, 17:3-12, 20:19-28, 21:7-24; SAMSUNG-1003, ¶[38].

[4] Houghton also refers to push clients as components 704, 804, 904, and 906.

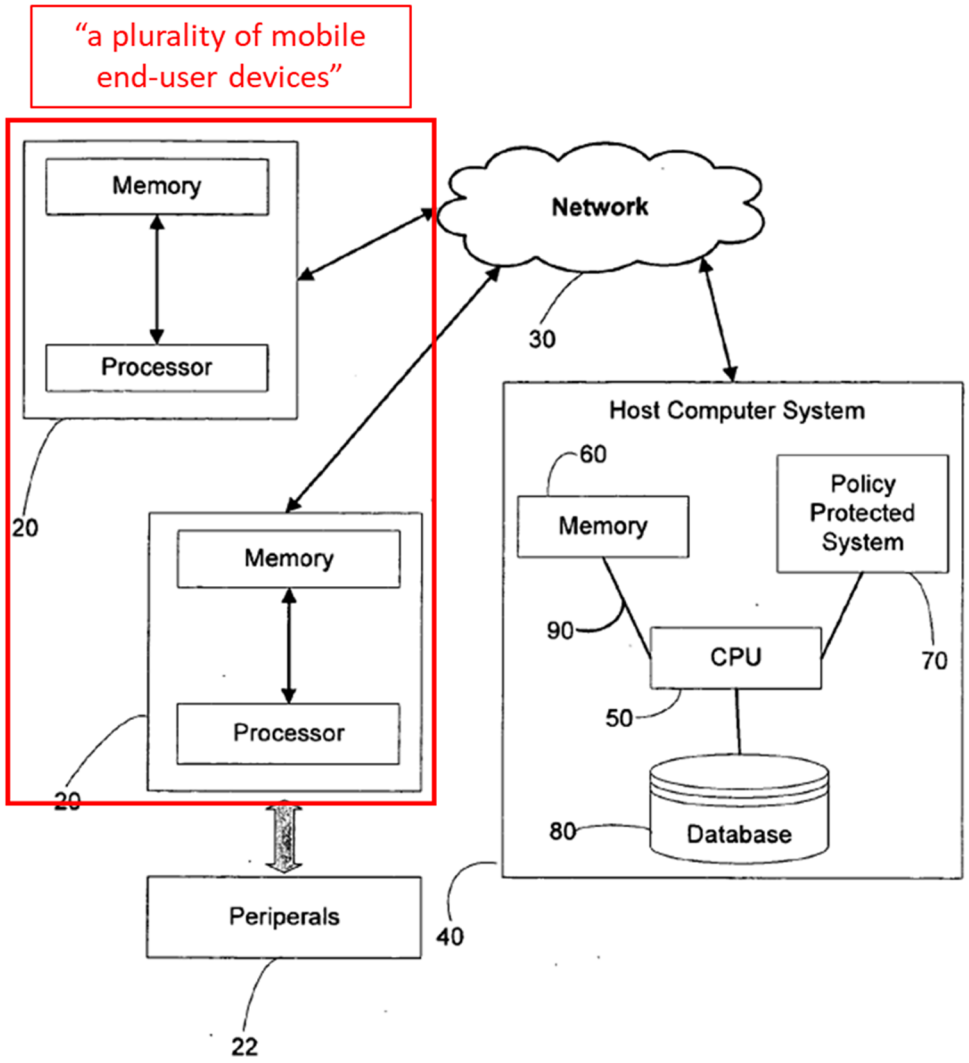
Figure 4



SAMSUNG-1005, FIG. 4 (annotated).

A POSITA would have recognized or found obvious by the Critical Date that network systems would have included a "***plurality***" of mobile terminals, each including its own "***device messaging agent***." SAMSUNG-1003, ¶[39]. Indeed, Houghton describes that events at "another" mobile terminal can trigger a push to a push client ("***plurality***" of push clients and terminals). SAMSUNG-1005, 14:8-11. Additionally, Houghton frequently refers to a plurality of "terminal**s**." SAM-

SUNG-1005, 18:16-27 ("Since there are numerous variations between mobile terminals and in network connectivity …"), 19:7-10 ("this reduces resource usage on the server when large number of mobile terminals is served"), 23:22 ("Referring now to Figure 5, users of mobile terminals 507 …"). Kalibjian also discloses a system with a plurality of "computing devices 20." SAMSUNG-1006, ¶[0010]-[0011], FIG. 1; SAMSUNG-1003, ¶[39].



SAMSUNG-1006, FIG. 1 (annotated).

Moreover, Munson provides corroboration, disclosing a content push service in communication with a plurality push clients. SAMSUNG-1007, 3:7-39, FIG. 2; SAMSUNG-1003, ¶[40].

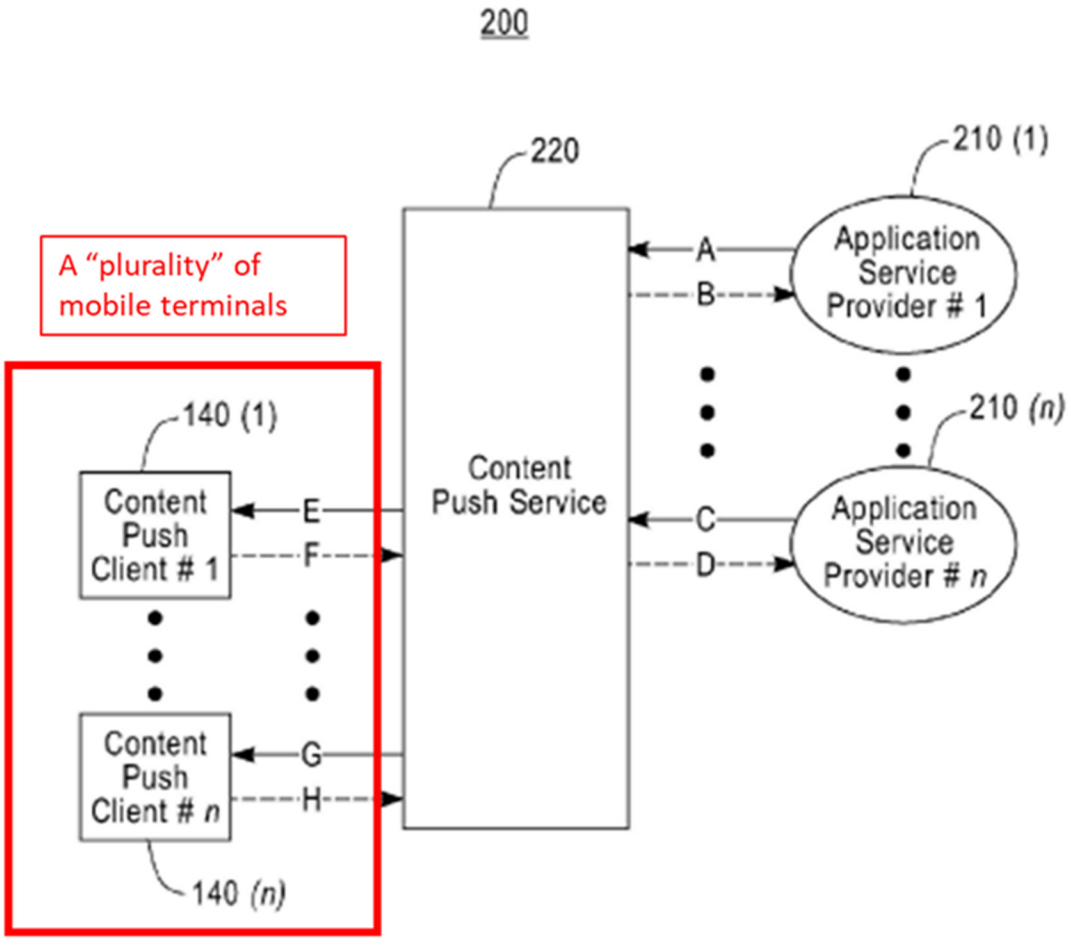


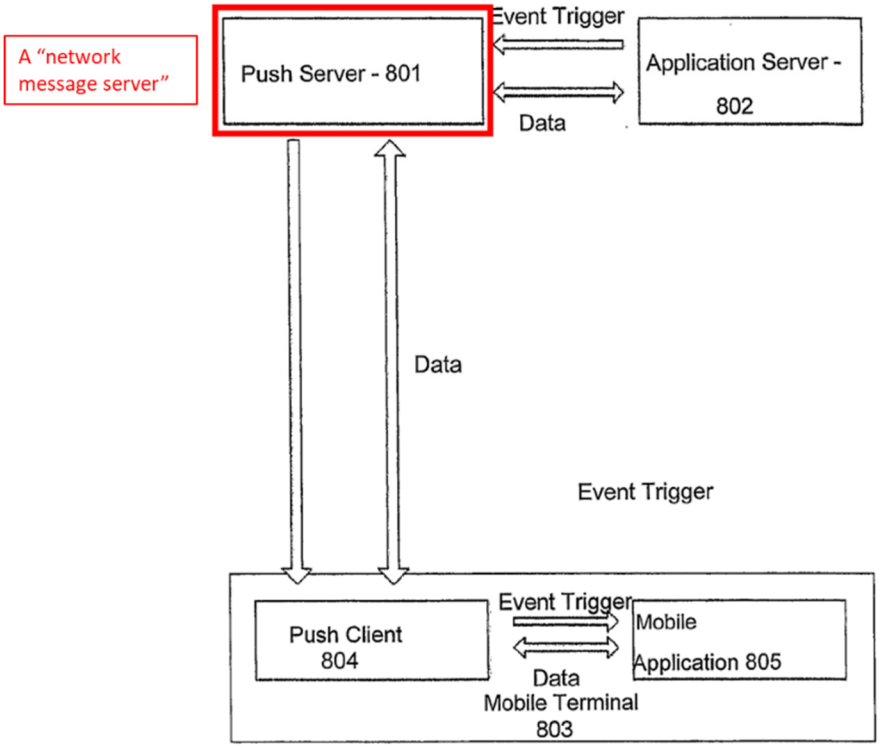
FIG. 2

SAMSUNG-1007, FIG. 2 (annotated).

Moreover, *In re Harza* held that "mere duplication of parts has no patentable significance unless a new and unexpected result is produced." 274 F.2d 669 (CCPA 1960).

[1.2]

Houghton discloses a "push server" ("***network message server***") in communication with the push clients. SAMSUNG-1005, 8:14-32, 16:16-35, 17:1-12, 21:35-36, 22:1-6, 23:3-22, 24:19-34, FIGS. 2-5, 7-9; *see supra* [1.1]. Presented below is Houghton's Figure 8, which depicts a push server 801[5] communicating with a push client 804 executing on a mobile terminal 803. *Id.*, FIG. 8; SAMSUNG-1003, ¶[41].



SAMSUNG-1005, FIG. 8 (annotated).

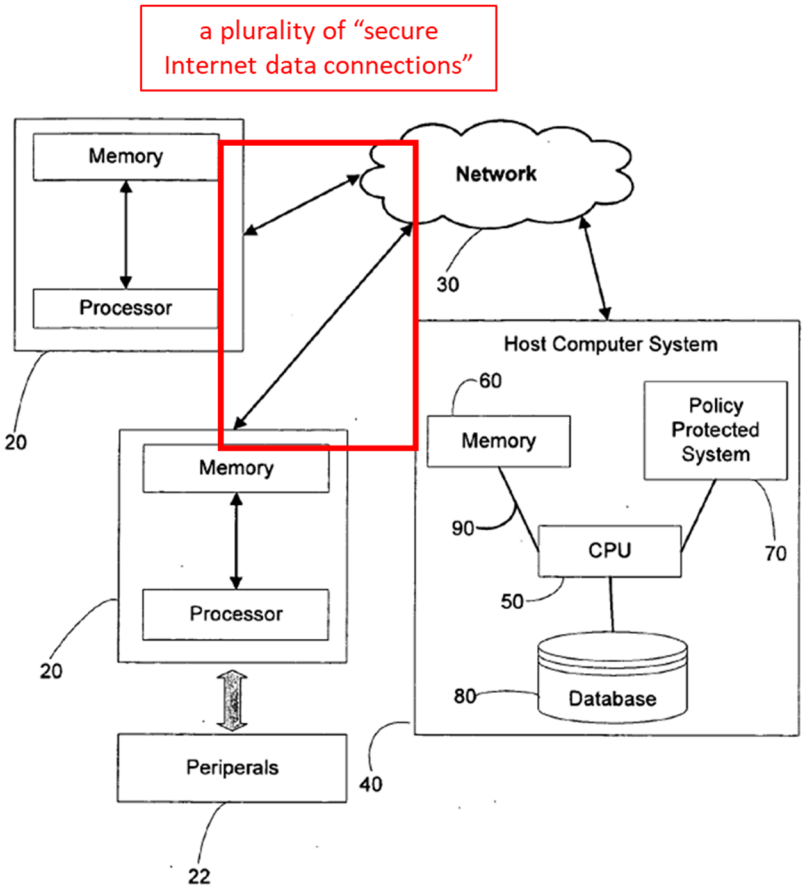
[5] Houghton also refers to push servers as components 202, 301, 401, 501, 701, and 901.

As illustrated above, Houghton's push client "attempts to log into the push server 401 over a data network 403," which is "a wireless network capable of transmitting Internet Protocol (IP) packets" ("***Internet data connections … between the network message server and a respective one of the mobile end-user devices via a device data connection to a wireless network***"). SAMSUNG-1005, 17:3-12. Houghton describes the connection between the push server and push client as "persistent managed, tested and configured" and that this connection can be implemented as "[a]n IP or other API (application programming interface)." SAMSUNG-1005, 23:3-21; SAMSUNG-1003, ¶[42].

Additionally, Houghton discloses various security protocols that are within the scope of its techniques. SAMSUNG-1005, 16:16-27, 19:14-17, 20:19-28. For example, Houghton discloses "secure protocol[s]" such as "HTTPS, IP-Sec, secure IP6 or a proprietary security protocol" and "SSL" ("***secure Internet data connections***"), which "identify the communicating parties, prevent message interception by 3rd parties, and prevent message modification by 3rd parties." *Id.*; SAMSUNG-1003, ¶[43].

A POSITA would have recognized or found obvious that Houghton's network system would have included a plurality of "***secure Internet data connections***" because it was known in the art that a server would be in communication with a plurality of mobile terminals and Houghton discloses that communication

occurs for a "plurality" of connections. SAMSUNG-1005, 7:3-7. Indeed, Houghton describes that events at "another" mobile terminal can trigger a push to a push client (a "***network message server***" is in communication with a "***plurality***" of push clients and terminals"). SAMSUNG-1005, 14:8-11; *see also id.* 9:8-10 ("one or more mobile terminals"), 21:25-34; *see supra* [1.1]. Additionally, Kalibjian also discloses a system with a plurality of "computing devices 20" in communication with a "network 30" (a plurality of "***secure Internet data connections***"). SAMSUNG-1006, ¶[0010]-[0013], FIG. 1; SAMSUNG-1003, ¶[44].



SAMSUNG-1006, FIG. 1 (annotated).

Munson corroborates that a "plurality" of such connections exists in a wireless network. SAMSUNG-1007, 1:48-56; FIG. 1; SAMSUNG-1003, ¶[45].

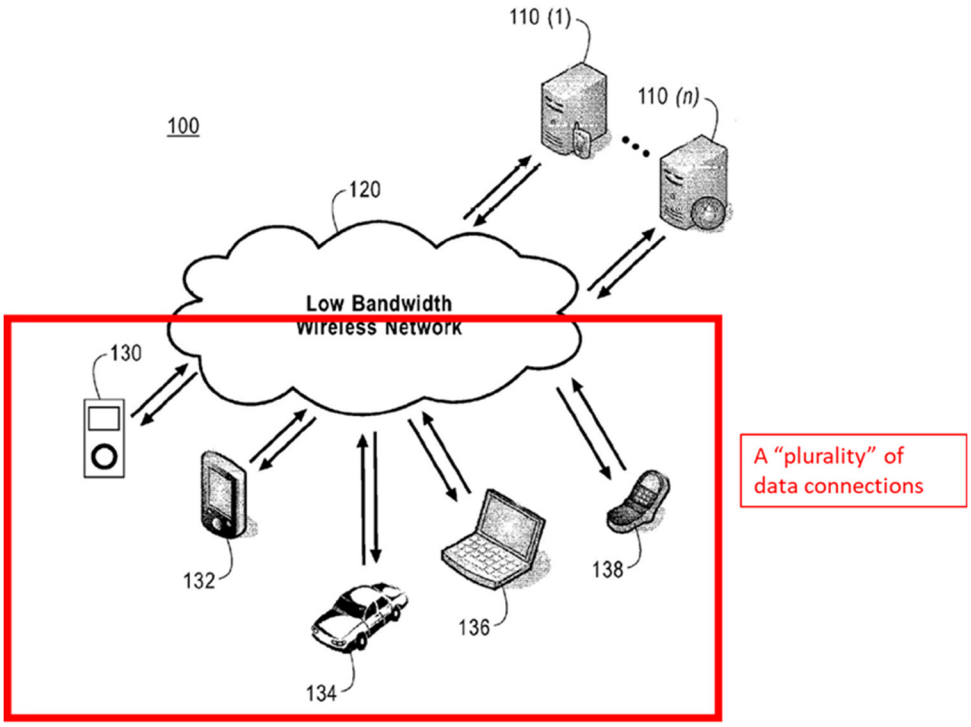


FIG. 1
Prior Art

SAMSUNG-1007, FIG. 1 (annotated).

Moreover, "mere duplication of parts has no patentable significance unless a new and unexpected result is produced." *In re Harza*, 274 F.2d 669.

[1.3]

Houghton discloses a "COMMAND PUSH" (hereafter, "command push") process in which an "application server 702[6]" pushes an "application command

[6] Houghton also refers to application servers as components 502, 802, and 902.

message" to a push client executing on the mobile terminal. SAMSUNG-1005, 21:35-36, 22:1-18, FIG. 7. Additionally, Houghton discloses this command push process, implemented by a "push server 701," is "triggered by a trigger event as for example … application server 702 to push an application command message to the push client 704" ("***receive[s], from each of a plurality of network application servers, multiple requests to transmit application data***"). SAMSUNG-1005, 16:15-21, 21:35-36, 22:1-18, FIG. 7; SAMSUNG-1003, ¶[46]. Houghton discloses that command messages "initiate a mobile terminal client trigger event in a mobile application 705 from a plurality of such applications" and that "[e]ach mobile application 205 has a fixed IP port number such as TCP/IP or UDP/IP" used to route the message to the application ("***each such request indicating … one of a plurality of applications***"). SAMSUNG-1005, 8:14-26, 21:35-36, 22:1-18, FIGS. 7-8; *see also id.* 16:15-21, 21:35-36, 22:1-18, 24:19-34. As Dr. Traynor explains, a POSITA would have recognized that "IP port numbers" would have additionally been unique to the mobile terminal ("***each such request indicating a corresponding one of the mobile end-user devices***") as IP addresses were (and still are) used as of the Critical Date to differentiate network locations (e.g., one mobile terminal from another). SAMSUNG-1003, ¶[46]. Indeed, Houghton corroborates Dr. Traynor's testimony and discloses that "IP-based technologies" use "IP address[es]" to indicate a particular terminal to receive a mobile push. SAMSUNG-1005, 1:10-18,

6:5-18; SAMSUNG-1003, ¶[46].

As Dr. Traynor explains, a POSITA also would have recognized or found obvious that the network message server would receive requests from a "***plurality of network application servers***" as this was well known in the art by the Critical Date. SAMSUNG-1003, ¶[47]. Indeed, Houghton describes a plurality of "content and application producers." SAMSUNG-1005, 14:28-31. Moreover, Kalibjian discloses that its "host computer system 40" (in communication with computing devices 20 over network 30) includes a plurality of "computers …, computer systems, mainframe computers, servers, distributed computing devices, and gateway computers." SAMSUNG-1006, ¶¶[0014]-[0015]. Additionally, Munson discloses a content push service in communication with a plurality of such application servers. SAMSUNG-1007, 1:48-56, 3:7-39, FIGS. 1-2; SAMSUNG-1003, ¶[47].

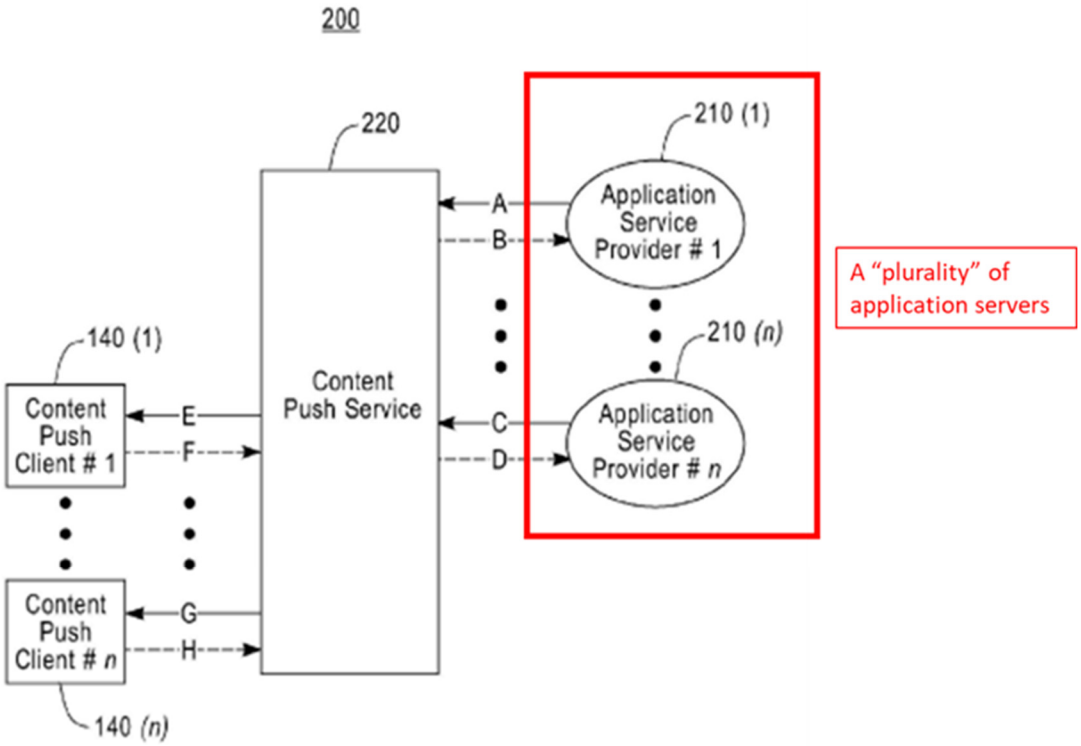


FIG. 2

SAMSUNG-1007, FIG. 2 (annotated).

Moreover, "mere duplication of parts has no patentable significance unless a new and unexpected result is produced." *In re Harza*, 274 F.2d 669.

[1.4]

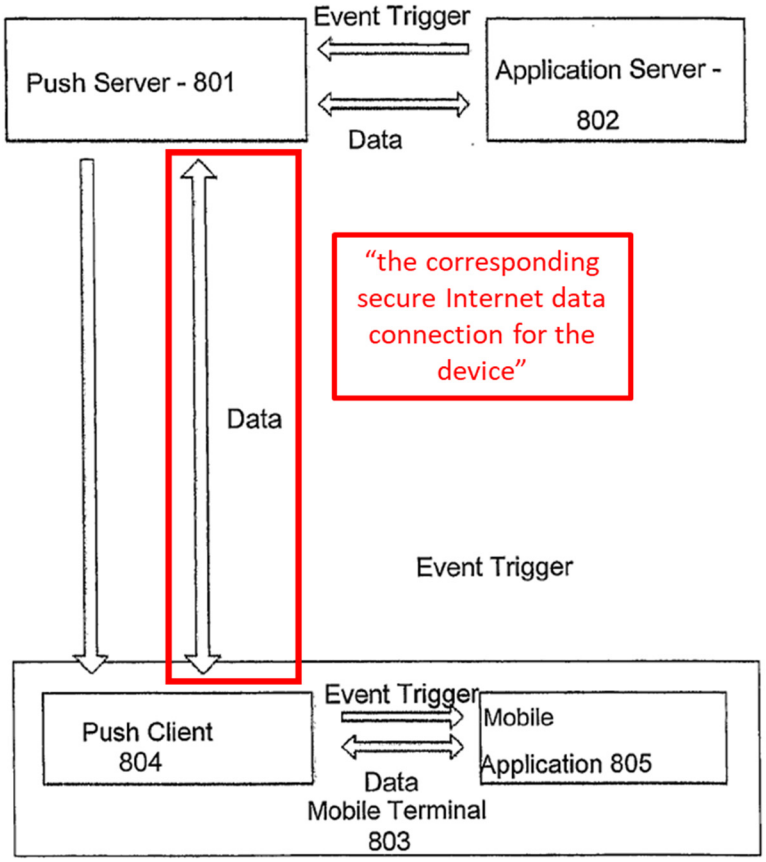
Houghton discloses that the push server generates "command" and "data push messages" for transmission over an IP protocol ("***Internet***") to the push client in response to a "trigger event" received from an "application server 702" ("***the network message server to generate corresponding Internet data messages based on the requests***"). SAMSUNG-1005, 16:16-27, 17:3-12, 19:14-17, 20:19-28,

21:7-22:18, 27:22-36, 28:1-3; *see supra* [1.2]. Trigger events include desired application functions (e.g., "an alarm, notification, or measurement result"), which the push server 401 packages into messages and transmits to the push client 405 (such that the messages are "***based on***" the trigger events). SAMSUNG-1005, 19:25-34. These messages include "data packet[s]," and may also include "[a]dditional binary or text information," for example, information "specifying how upon receiving such a message the client 405 will notify [the user]" ("***application data corresponding to one of the requests***"). *Id*., 21:7-34. Houghton's push messages include "[a]dditional binary or text information specifying which mobile application 406 from a plurality of such applications" ("***each such message containing at least one application identifier for an indicated application***"). *Id*., 21:7-34; SAMSUNG-1003, ¶[48].

As Dr. Traynor explains, a POSITA would have also recognized or found obvious that "***each***" message generated by the network message server would contain an "***application identifier***" and "***application data***" because, without either, the generated message would be meaningless. SAMSUNG-1003, ¶[49] ("[a] message without an application identifier would leave the device messaging agent with no instructions on where to send the received data, and a message with only an application identifier and no application data would be pointless").

[1.5]

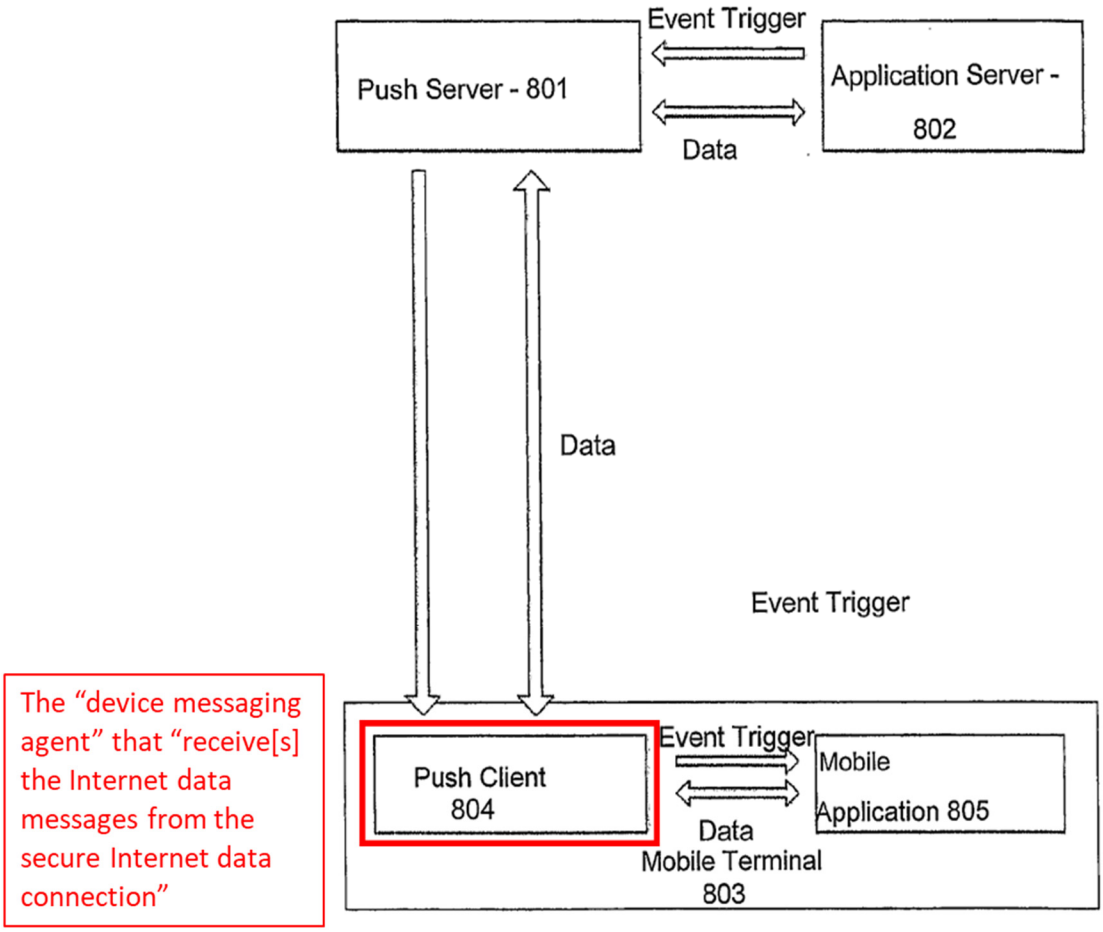
Houghton discloses that messages are "pushed" from "server 401" to "client 405" ("***the network message server to transmit each of the generated Internet data messages to the device messaging agent located on the device***"). SAMSUNG-1005, 20:19-28, 21:7-24. As described above in [1.3], the IP addresses used by Houghton would have indicated the device (and therefore the push client) to receive the push messages ("***the device indicated in the corresponding request***"). SAMSUNG-1005, 1:10-18, 6:5-18, 8:14-26; *see supra* [1.3]. Additionally, Houghton discloses a "persistent managed, tested and configured data connection … between push server 401/801 and push client 405/804" ("***using the corresponding secure Internet data connection for the device indicated in the corresponding request***"). SAMSUNG-1005, 23:3-21, FIGS. 2-5, 7-9; *see supra* [1.2]; SAMSUNG-1003, ¶[50].



SAMSUNG-1005, FIG. 8 (annotated).

[1.6]

Each of Houghton's "push client[s]" receive message traffic from the "push server" intended for their corresponding mobile terminal ("***each device messaging agent, when executing, to receive the Internet data messages from the secure Internet data connection corresponding to the device executing the device messaging agent***"). SAMSUNG-1005, 20:19-28, 21:7-24, FIGS. 2-5, 7-9; *see supra* [1.2], [1.5]; SAMSUNG-1003, ¶[51].



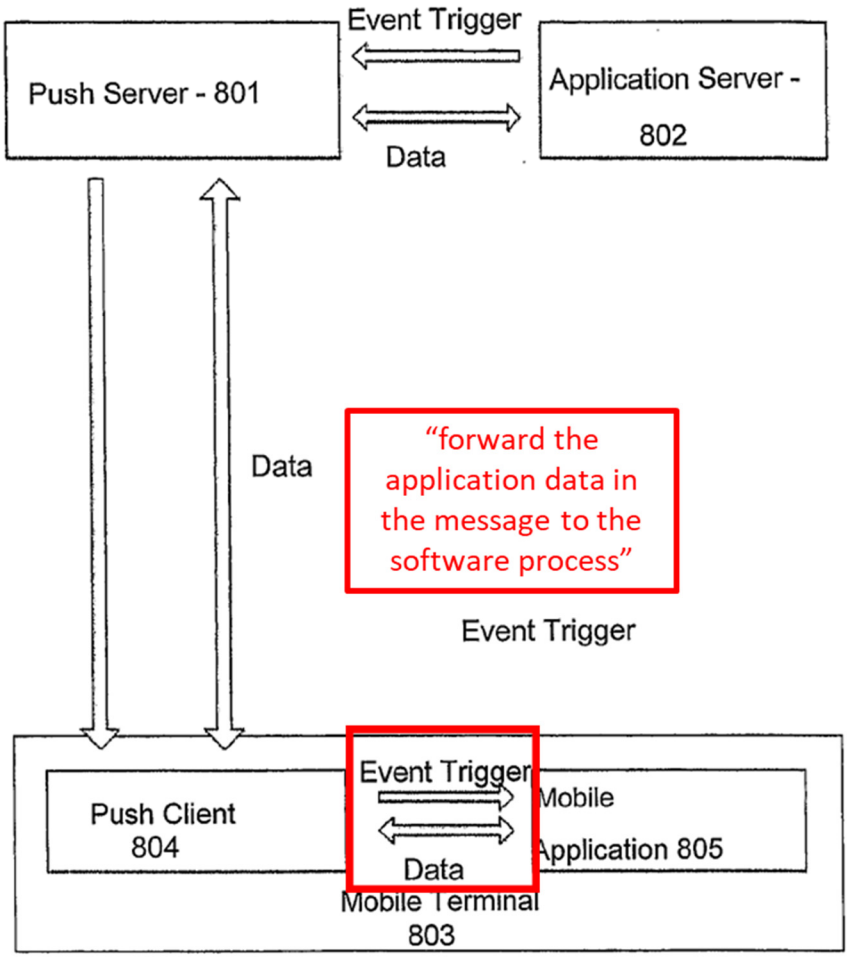
SAMSUNG-1005, FIG. 8 (annotated).

[1.7]

Houghton discloses that messages include "[a]dditional binary or text information specifying which mobile application 406 from a plurality of such applications" should receive the message. SAMSUNG-1005, 21:7-24, FIGS. 2-5, 7-9; *see supra* [1.3], [1.6]. For example, as described above in [1.3], Houghton's push messages include IP address information that is mapped to a "fixed IP port number" that corresponds to an application ("***map the application identifier in the***

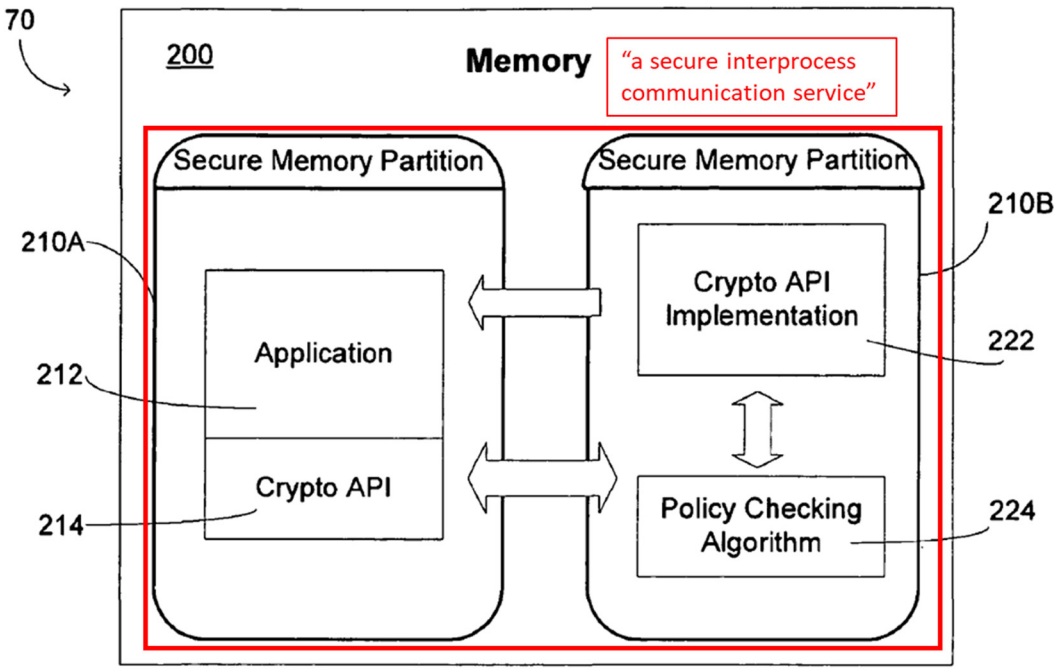
message to a software process corresponding to the application identifier").

SAMSUNG-1005, 8:14-26; *see supra* [1.3]. After receiving a message, "appropriate automated actions and user interface media capabilities of the mobile terminal … are executed by the push client 405" to include "passing the command details … to the specified mobile application" ("***forward the application data in the message to the software process***"). *Id.*; SAMSUNG-1003, ¶[52]. As evident in FIG. 8 below, data from messages received by the push client is passed to an application.

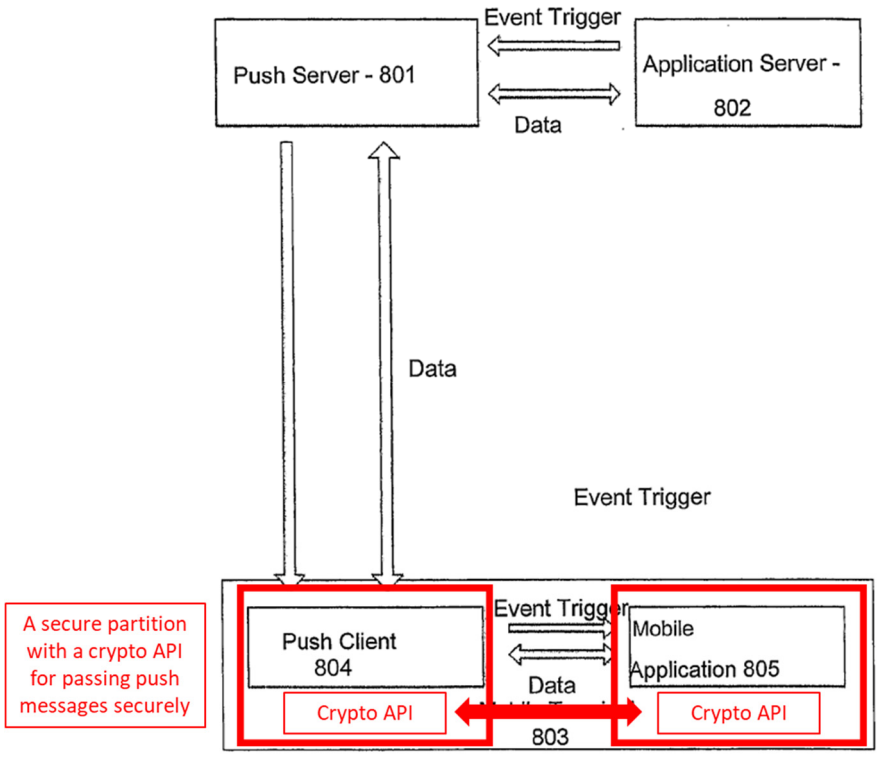


SAMSUNG-1005, FIG. 8 (annotated).

Kalibjian discloses a device where a memory is divided into "separate and distinct secure sections" with applications that "[make] API requests or calls via a secure messaging paradigm" ("***a secure interprocess communication service***"). SAMSUNG-1006, ¶¶[0019]-[0021]; *see also* SAMSUNG-1001, 42:45-67, 43:1-4. Kalibjian further discloses that, when applications make requests, a "policy checking algorithm 224 evaluates the request with respect to the established security policy" and permits the communication if it is allowed. SAMSUNG-1006, ¶[0021]. These security policies can include "cryptographic algorithms to use, key sizes, allowable hash algorithms, etc." *Id*. In the Houghton-Kalibjian combination, one example of which is illustrated below, secure memory sections, policy checking, and crypto APIs based on the disclosure of Kalibjian would have been incorporated into the mobile terminal of Houghton, such that messages received by Houghton's push client (executing in a secure memory section) would be securely passed to the destination application (executing in another secure memory section) ("***a secure interprocess communication service***"). SAMSUNG-1005, 23:3-21, FIGS. 2-5, 7-9; SAMSUNG-1006, ¶¶[0019]-[0021], FIG. 2; *see supra* §III.A.3; SAMSUNG-1003, ¶[54].



SAMSUNG-1006, FIG. 2 (annotated).



SAMSUNG-1005, FIG. 8 (annotated).

Additionally, as Dr. Traynor explains, the '117 Patent does not define "***a secure interprocess communication service***," but instead generally lists various features of secure communication. SAMSUNG-1001, 42:45-67, 43:1-4; SAMSUNG-1003, ¶[53]. Accordingly, the implementation of security features that satisfy at least one of the many embodiments of a ***"secure interprocess communication service***" according to the '117 Patent would have largely been left to the general knowledge and capabilities of a POSITA (e.g., by incorporating the use of Kalibjian's secure memory sections and crypto APIs in Houghton's push message system). SAMSUNG-1003, ¶[53]; *see supra* III.A.3.

[3]

Houghton discloses that its system is compatible with a variety of mobile terminal operating systems, to include "Symbian, Linux, [and] Microsoft." SAMSUNG-1005, 8:14-26. As Dr. Traynor explains, a POSITA would have recognized that these different operating systems and their associated applications would have required "***application data***" in various "***formats***" (at least "***a first application that receives the application data in a first format, and a second application that receives the application data in a second format***"). SAMSUNG-1005, 8:14-26; SAMSUNG-1003, ¶[55]. Indeed, Houghton corroborates Dr. Traynor's testimony and discloses different software processes that can be invoked by Houghton's "trigger events." SAMSUNG-1005, 21:35-22:18; SAMSUNG-1003, ¶[55].

Houghton additionally discloses different types of applications and services (a "***plurality of applications***") that trigger "IP command push messages" to include:

> … the making, receiving, and termination of telephone calls, the transition from presence-to-absence or absence-to-presence of other devices in a geographical area, metropolitan area, local area or personal area wireless communications network, mobile terminal creation of photographs video audio or other media, mobile terminal presence of files matching a given filtering criteria, changes in internal state of electronic equipment, taking of measurements, processing of such measurements to see if they match certain criteria, video game actions or events, application calculation events and messaging actions.
>
> SAMSUNG-1005, 14:8-27; SAMSUNG-1003, ¶[56].

As Dr. Traynor explains, a POSITA would have recognized or found obvious that the above applications and services would require "application data" in at least a "first format" and a "second format" because a POSITA would have known the above applications require different communication formats (e.g., a "video game" application would require a different push message format than a "messaging" application). SAMSUNG-1003, ¶[57].

[4]

As an initial matter, Dr. Traynor explains that this claim "recites only basic encryption/decryption without any additional detail," and as such, a POSITA would have found it obvious for multiple reasons. SAMSUNG-1003, ¶[58].

First, Houghton discloses multiple secure protocols such as "HTTPS, IP-Sec, [and] secure IP6." SAMSUNG-1005, 17:13-25, 19:14-17. Moreover, Houghton discloses that operators of push services "control" and "encrypt" traffic ("***encrypt the secure Internet data messages***"). SAMSUNG-1005, 3:22-33. For example, using the HTTPS protocol, the push server of Houghton would have encrypted messages sent to the push client over the "***secure Internet data connection***" (e.g., an IP-Sec connection). SAMSUNG-1005, 3:22-33, 17:13-25, 19:14-17; SAMSUNG-1010, pp. 64-109 (disclosing the encryption techniques of TLS, which is used by HTTPS). As Dr. Traynor explains, "multi-layer encryption ('***the network message server further to encrypt the secure Internet data messages***') would have been achievable, for example, through the use of both HTTPS and IP-sec in combination." SAMSUNG-1005, 17:13-25, 19:14-17; SAMSUNG-1003, ¶[59]; *see supra* [1.2], [1.4]-[1.5].

Second, Dr. Traynor explains that it would have been obvious to a POSITA that Houghton's push server ("***network message server***") and push client ("***device messaging agent***") would perform encryption/decryption because (1) this would

prevent multiple components/applications from needing to perform encryption as the push server/client are central to push communication, and (2) it was known in the art by the Critical Date that push servers performed such encryption. SAMSUNG-1003, ¶[60]. Chou is one example of a push message system that uses a "WAP gateway" (e.g., a network message server) that encrypts content received from a "content server" for transmission to a "mobile client" that then "decodes the response." SAMSUNG-1009, ¶¶[0054]-[0060]. Rakic and Shen provide additional examples of a push server encrypting message traffic. SAMSUNG-1008, ¶¶[0065]-[0068]; SAMSUNG-1025, ¶¶[0056]-[0060], FIG. 5; SAMSUNG-1003, ¶[60].

Third, Kalibjian discloses that "messages or requests" can include "a particular cryptographic key size or a particular cryptographic algorithm or hashing algorithm." SAMSUNG-1006, ¶[0029]. Thus, the encryption methods of Kalibjian would have served as additional implementation examples for message encryption when combined with Houghton's existing encryption techniques. SAMSUNG-1005, 3:22-33, 17:13-25, 19:14-17; SAMSUNG-1003, ¶[61].

Dr. Traynor explains that, in each of the above examples, a POSITA would have recognized or found obvious that, in decrypting the messages, the push client would "***obtain the corresponding application identifier and application data***" because this information is included in the encrypted message. SAMSUNG-1003,

¶[62].

[5]

As Dr. Traynor explains, a POSITA would have recognized or found obvious that "***the secure Internet data messages are transported to the device messaging agent***" using "***one or more of encryption on a transport services stack, [and/or] IP (Internet Protocol) layer encryption***" because these techniques are within the secure protocols described by Houghton. SAMSUNG-1005, 17:13-25, 19:14-17; SAMSUNG-1010, pp. 100-103; SAMSUNG-1003, ¶[63]; *see supra* [4]. For example, the "IPsec" protocol described above in [4] is an end-to-end security scheme that is "***encryption on a transport services stack***" and "***IP (Internet Protocol) layer encryption***." SAMSUNG-1005, 17:13-25, 19:14-17; *see supra*, [4]; SAMSUNG-1003, ¶[63]. As another example, the "[Hypertext Transfer Protocol Secure] HTTPS protocol" described above in [4] is encrypted using Transport Layer Security (TLS) ("***encryption on a transport services stack***" and "***IP (Internet Protocol) layer encryption***"). SAMSUNG-1005, 17:13-25, 19:14-17; SAMSUNG-1010, pp. 100-103; *see supra* [4]; SAMSUNG-1003, ¶[63]. Additionally, Anderson (a network security textbook) discloses that IPsec is "widely used" by vendors who offer "virtual private network (VPN)" services ("***tunneling***"). SAMSUNG-1010, pp. 100-101. Based on Houghton's disclosure of using security pro-

tocols (e.g., IPsec and HTTPS) and a POSITA's general knowledge of security options available for Internet data messages, a POSITA would have found it obvious to transmit the push messages in Houghton using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling. SAMSUNG-1003, ¶[63].

[6]

Dr. Traynor explains that a POSITA would have recognized or found obvious that the push client of Houghton-Kalibjian would have communicated to applications outside of its ***secure execution environment*** (e.g., the terminal operating system) because Houghton refers to "basic terminal operating system software and programs installed by service providers." SAMSUNG-1005, 1:18-36, 2:1-6; SAMSUNG-1003, ¶[64]. For example, Houghton discloses that "mobile terminal operating systems also support remote application launch based on receipt of a text message." SAMSUNG-1005, 1:29-36, 2:1-6. To effectuate launching an application from a received message, the push client would have communicated with the mobile terminal operating system ("***outside of the secure execution environment***" of the push client). SAMSUNG-1005, 1:29-36, 2:1-6. Indeed, the need for both normal and secure execution environments is corroborated by Ellison, which discloses that applications can be executed in either environment. SAMSUNG-1013, 4:65-67, 5:1, 6:1-26, FIGS. 1A, 1C; SAMSUNG-1003, ¶[64].

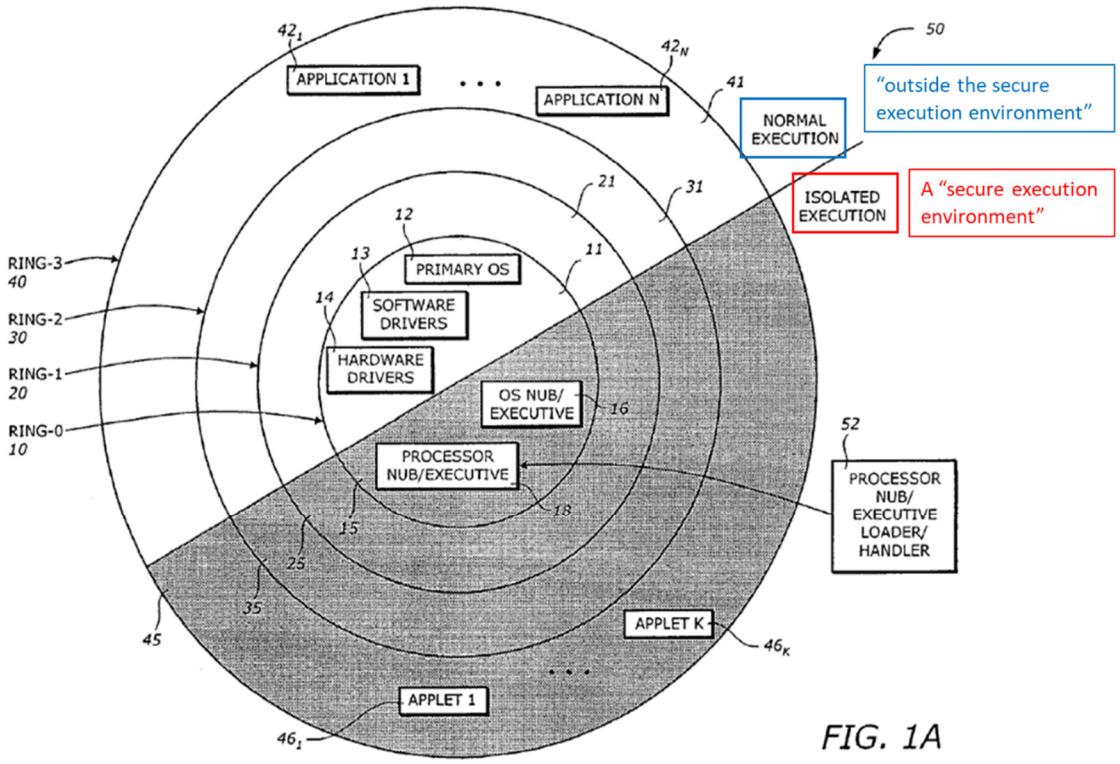
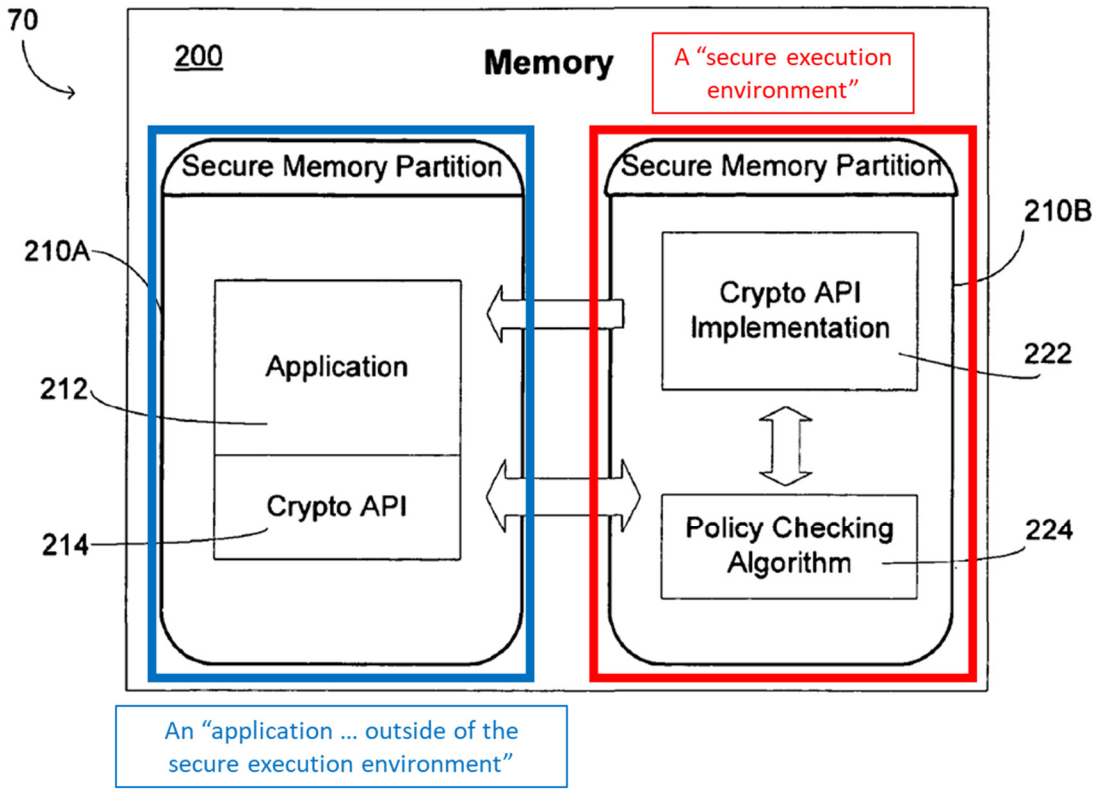


FIG. 1A

SAMSUNG-1013, FIG. 1A (annotated).

Additionally, Kalibjian discloses a "secure memory" with "two separate and distinct secure sections" that include "an application or applications 212" and a "policy checking application or algorithm 224." SAMSUNG-1006, Abstract, ¶¶[0019]-[0021], FIG. 2. In the Houghton-Kalibjian combination, the push client would have been incorporated into one of these secure sections ("***the device messaging agent executes in a secure execution environment***"), with groupings of applications incorporated into other secure sections ("***at least one of the applications***

executes outside of the secure execution environment")[7]. SAMSUNG-1006, Abstract, ¶¶[0019]-[0021], FIG. 2; *see supra* §III.A.3; SAMSUNG-1003, ¶[65].

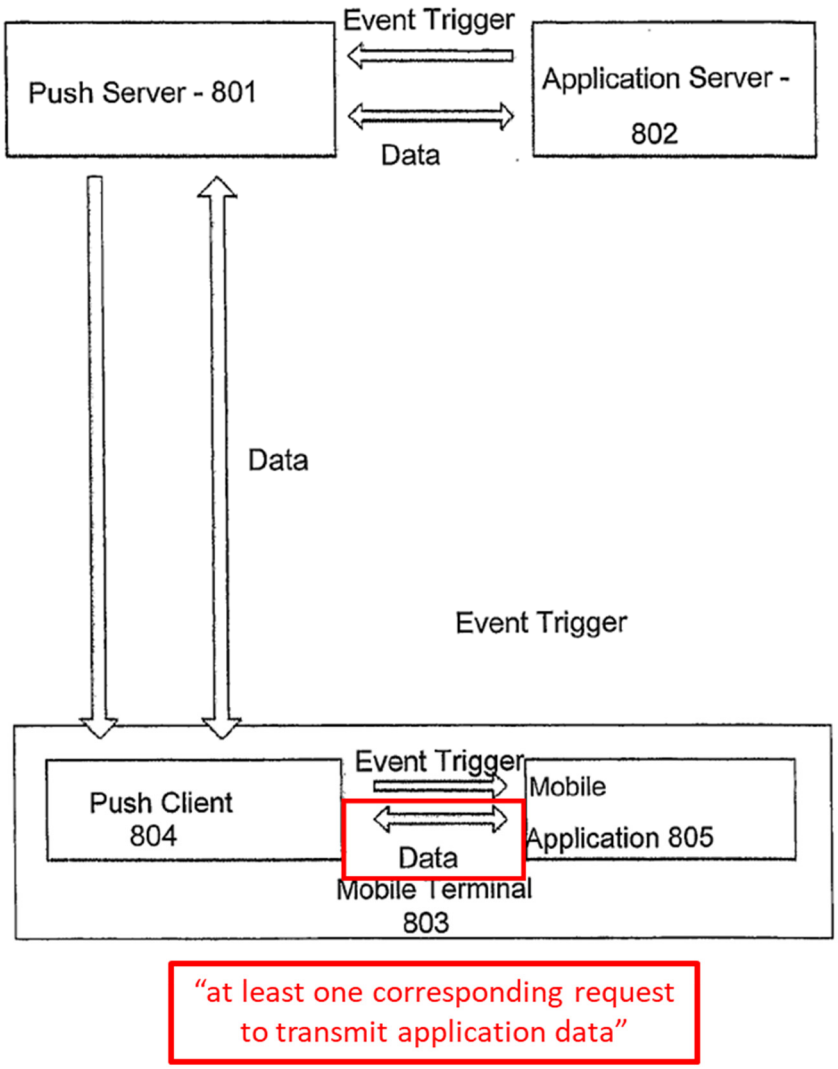


SAMSUNG-1006, FIG. 2 (annotated).

[7] The antecedent basis for this claim requires that the applications operate outside of the secure execution environment of the device messaging agent. This does not preclude the applications from being executed in another secure execution environment.

[7.1]

Houghton discloses a "command push with bidirectional data" where communication flows from the mobile terminal to the application server. SAMSUNG-1005, 23:3-21, FIG. 8. As evident in FIG. 8, the requests to transmit data from the applications are received by the push client 804 ("***at least a subset of the device messaging agents, when respectively executing on their respective devices, are each further to receive, from each of multiple applications executing on the corresponding device, at least one corresponding request to transmit application data***"). *Id*. As Dr. Traynor explains, a POSITA would have recognized or found obvious that the requests to transmit data would have "***indicat[ed] a corresponding one of the network application servers***" because the push client 804 and push server 801 would have needed this information to route the upload to the correct destination. SAMSUNG-1005, 23:3-21, FIG. 8; SAMSUNG-1003, ¶[66]. Indeed, Munson corroborates Dr. Traynor's testimony and discloses a system where, once a push message is received, "acknowledge receipts" are sent to the "application service providers" that sent the push message. SAMSUNG-1007, 3:15-20. As Dr. Traynor explains, "to transmit an acknowledgement using, for example, Houghton's bi-directional 'command push,' the push client would have included IP address information indicating the network location of the application server." SAMSUNG-1005, 1:10-18, 6:5-18; SAMSUNG-1003, ¶[66]; *see supra* [1.3].



SAMSUNG-1005, FIG. 8 (annotated).

[7.2]

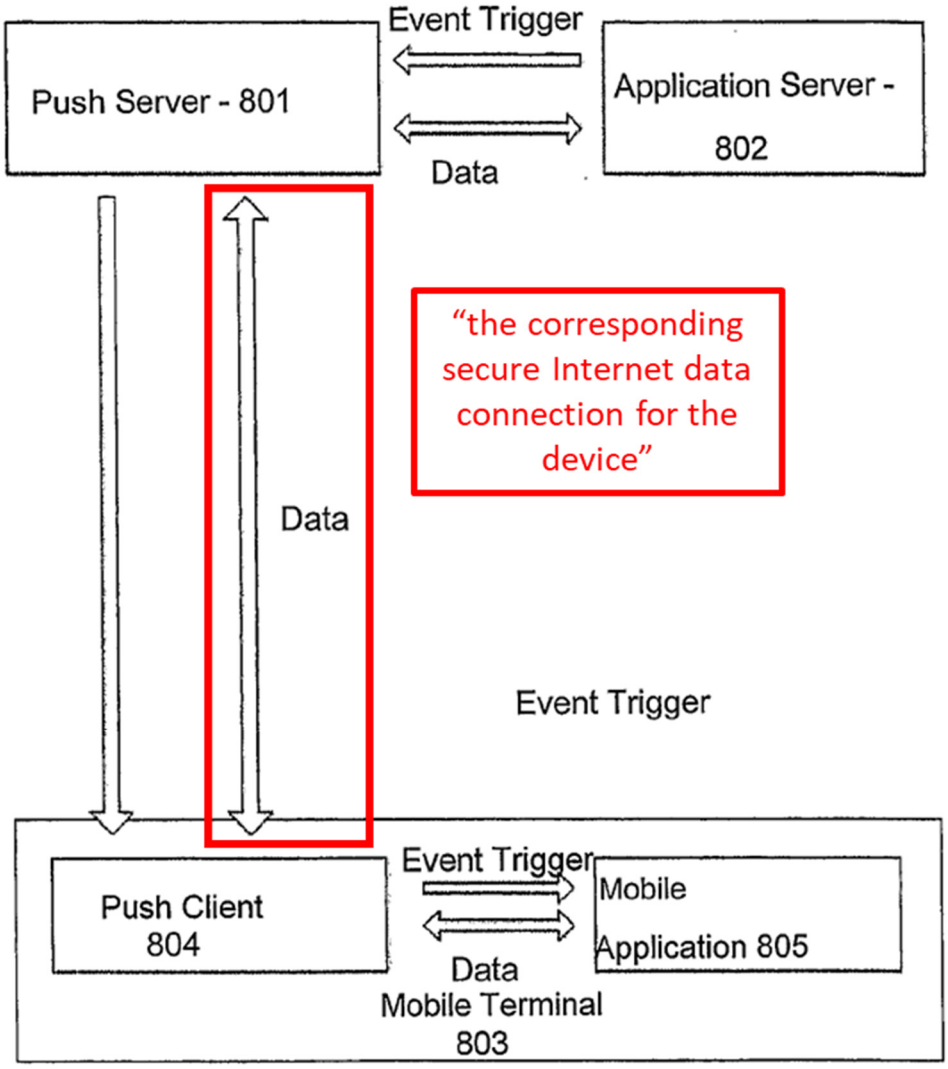
As discussed in [7.1], the data messages would have "***contain[ed] at least one server identifier for an indicated application server and application data corresponding to one of the requests***." *See supra* [7.1]; SAMSUNG-1003, ¶[67].

Dr. Traynor explains that a POSITA would have recognized or found obvious that the push client 804 would have "generate[d] corresponding upload Internet

data messages based on the requests" as FIG. 8 depicts the push client 804 transmitting application data to the push server 801. SAMSUNG-1005, FIG. 8; SAMSUNG-1003, ¶[68]. Additionally, Houghton discloses that its command push messages are "a data connection between application server 802 and mobile application 805" ("***an indicated application server and application data corresponding to one of the requests***"). SAMSUNG-1005, 23:3-21, FIG. 8; *see supra* [1.3]-[1.4]; SAMSUNG-1003, ¶[68].

[7.3]

As depicted in FIG. 8, the push client 804 transmits data uploads to the push server 801 ("***transmit each of the generated upload Internet data messages to the network message server***"). SAMSUNG-1005, FIG. 8. As Dr. Traynor explains, a POSITA would have recognized or found obvious that the push client 804 would use "***the corresponding secure Internet data connection for the device***" because Houghton discloses a "persistent managed, tested and configured data connection" between the push server 801 and push client 804. SAMSUNG-1005, 23:3-21, FIG. 8; *see supra* [1.2] and [7.1]-[7.2]. Moreover, Houghton discloses that "the push server 401 sends the client 405 push commands or data and may return response through the same IP connection." SAMSUNG-1005, 28:1-3; SAMSUNG-1003, ¶[69].



SAMSUNG-1005, FIG. 8 (annotated).

[7.4]

Houghton discloses that the bi-directional "command push" includes a "configured data connection … between push server 401 /801 and push client 405/804." SAMSUNG-1005, 23:3-21. As evident in FIG. 8, the transmitted data upload messages are received by the push server 801 ("***the network message server is further to receive the upload Internet data messages over the respective secure Internet***

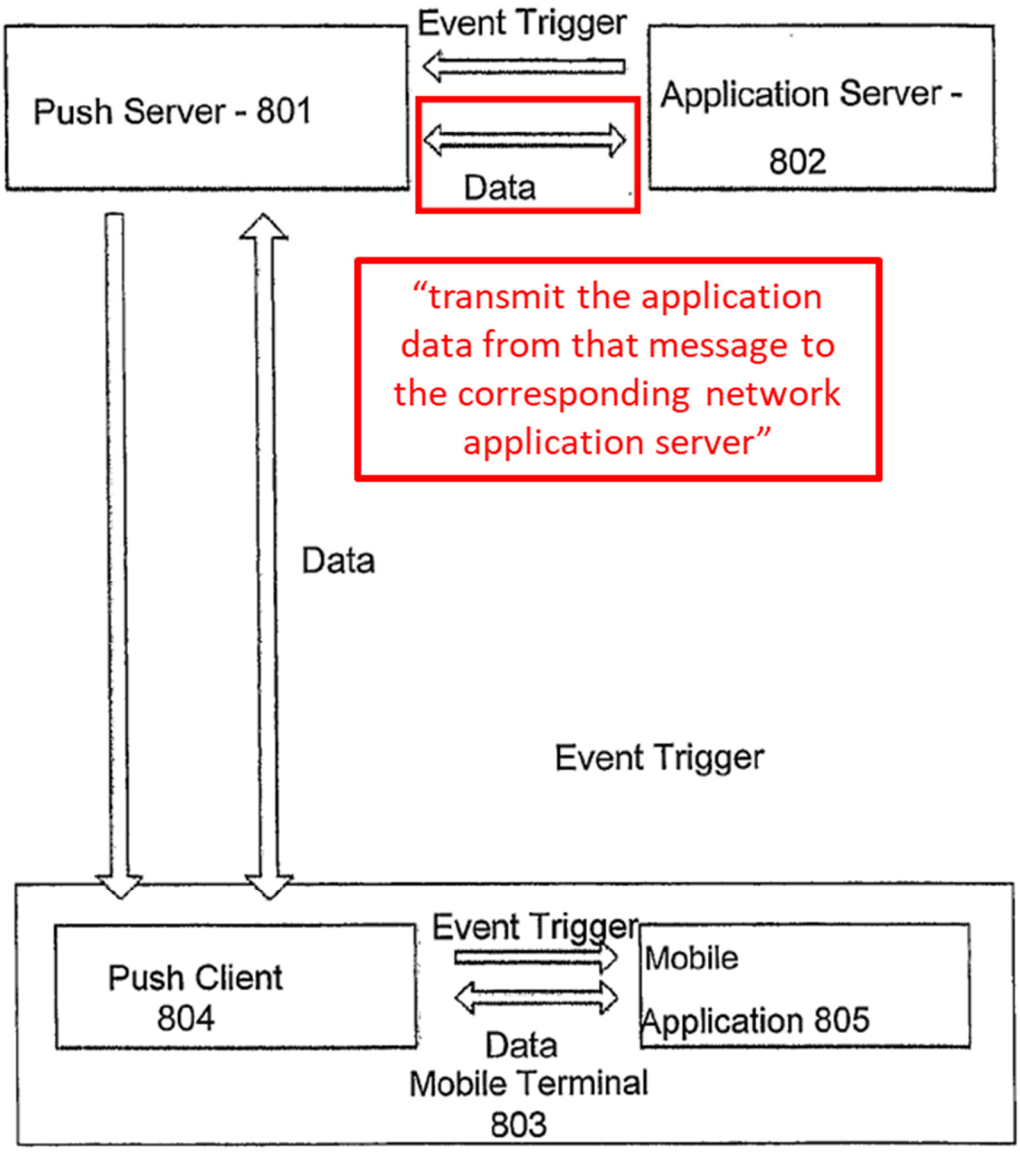
data connections"). SAMSUNG-1005, FIG. 8; *see supra* [7.3]; SAMSUNG-1003, ¶[70].

[7.5]

As depicted in FIG. 8, the push server 801 "***transmit[s] the application data from that message to the corresponding network application server***." SAMSUNG-1005, FIG. 8; *see supra* [7.3]-[7.4]. Dr. Traynor explains that a POSITA would have recognized or found obvious that the push server 801 would have "***map[ped] the server identifier in that message to a corresponding one of the network application servers***" because this information would have been required to identify the particular application server to receive the data in the message. SAMSUNG-1003, ¶[71]; SAMSUNG-1005, FIG. 8.

Dr. Traynor further explains that a POSITA would have recognized or found obvious that the message to the application server would have contained "***an indication of the device from which that message was received***" because the application server is in communication with many such mobile terminals and would have needed to identify the specific mobile terminal that corresponded to the data. SAMSUNG-1003, ¶[72]. Indeed, Houghton discloses that the bidirectional command push data connection is between "application server 802 and mobile application 805" (operating on a particular mobile terminal 803). SAMSUNG-1005, 23:3-

21. Moreover, Munson corroborates Dr. Traynor's testimony and discloses a system where, once a push message is received, "acknowledge receipts" are sent from the receiving device to the "application service providers" that sent the push message. SAMSUNG-1007, 3:15-20; SAMSUNG-1003, ¶[72].



SAMSUNG-1005, FIG. 8 (annotated).

[8]

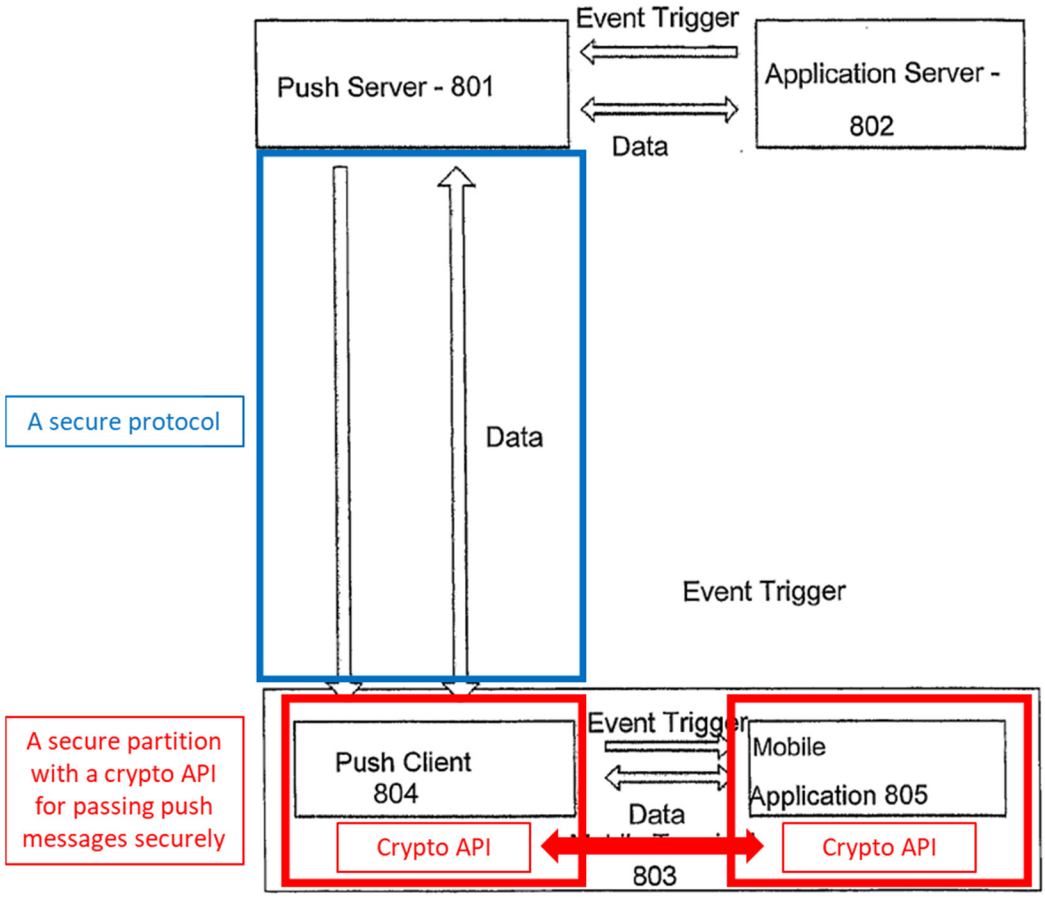
As Dr. Traynor explains, a POSITA would have recognized or found obvious that the messages transmitted from the Houghton-Kalibjian mobile terminal would contain a "***key for the application server***" because this would have increased the security of the push message system and enabled client-server authentication, a priority of Houghton. SAMSUNG-1005, 23:3-21 (a "persistently managed, tested and configured data connection"); SAMSUNG-1003, ¶[73]; *see supra* [7]. Indeed, Anderson provides an example implementation of TLS protocol authentication (an implementation of the HTTPS protocol Houghton describes) where the client sends a "***key*** exchange message" containing a "pre-master-secret ***key***" in order to share sensitive data with a server. SAMSUNG-1010, pp. 101-102. Dr. Traynor further explains that it would have been obvious to a POSITA that this key would be ***for the application server*** because "anything less would result in network security vulnerabilities that would have defeated the entire purpose of performing authentication and encryption in the first place." SAMSUNG-1003, ¶[73].

Kalibjian also discloses that "[t]he security policy can also specify particular attributes of the messages or requests" to include "a particular cryptographic key size or a particular cryptographic algorithm or hashing algorithm (such as SHA-1 or MD-5) ("***at least one of the upload Internet data messages comprises a key for the network application server corresponding to the requesting application***").

SAMSUNG-1006, ¶[0029]. As described above, Houghton already employs various encryption protocols. *See supra* [1.2], [4]-[5]; SAMSUNG-1003, ¶[74].

[9]

Houghton discloses the use of "secure protocols" to communicate between push servers and clients. SAMSUNG-1005, 19:14-17; *see supra* [1.2], [4]-[5]. Kalibjian discloses "an application in a first secure memory partition" that transmits a "request from the application to a cryptographic application programming interface (API)" which is then "[verified in a] second secure memory partition." SAMSUNG-1006, Abstract, ¶¶[0019]-[0021], FIG. 2; *see supra* [6]. Given the use of these two different methods of security, in the Houghton-Kalibjian combination, "***the secure interprocess communication service and the secure Internet data connection from that device to the network message server are separately secured***." SAMSUNG-1005, 19:14-17; SAMSUNG-1006, Abstract, ¶¶[0019]-[0021], FIG. 2; *see supra* [1.2], [4]-[6]; SAMSUNG-1003, ¶[75].



SAMSUNG-1005, FIG. 8 (modified to incorporate Kalibjian).

[10]

As Dr. Traynor explains, a POSITA would have recognized or found obvious that messages received from the push server would have been directed to multiple applications from among the "plurality" of applications ("***multiple identifier/data pairs***") because Houghton discloses various "actions" that occur across applications when receiving a push message. SAMSUNG-1005, 21:7-24; SAMSUNG-1003, ¶[76]. Indeed, Houghton corroborates Dr. Traynor's testimony and

discloses that, in some cases, the "packaging of mobile applications involves combining multiple applications delivered in a single bundle" (e.g., a "bundle" or "suite" of applications would receive messages packaged together – a message containing "***multiple identifier/data pairs***"). SAMSUNG-1005, 12:14-29; SAMSUNG-1003, ¶[76].

Moreover, "mere duplication of parts has no patentable significance unless a new and unexpected result is produced." *In re Harza*, 274 F.2d 669.

[11]

Kalibjian discloses that "[t]he security policy can also specify particular attributes of the messages or requests" to include "a particular cryptographic key size or a particular cryptographic algorithm or hashing algorithm (such as SHA-1 or MD-5). SAMSUNG-1006, ¶[0029]. Additionally, Kalibjian discloses that, when passing messages between memory partitions (e.g., the push agent to the application), the cryptographic API 214 "formats, encodes, or encrypts the request to comply with a pre-established communication protocol" ("***the secure interprocess communication service forwards the application data to at least one of the software processes in an encrypted format***"). SAMSUNG-1006, ¶¶[0024]-[0026]; SAMSUNG-1003, ¶[77].

As described above, Houghton already employs various encrypted protocols,

some of which provide end-to-end encryption. *See supra* [1.2], [4]-[5], [8]; SAMSUNG-1003, ¶[78]. Moreover, as Dr. Traynor explains, end-to-end encryption in messaging applications (e.g., the server to the application) was well known as of the Critical Date. SAMSUNG-1003, ¶[78]. Indeed, CryptoGraf, released in July 2007 for the Symbian and Windows Mobile operating systems, was one such secure messaging application. SAMSUNG-1015; SAMSUNG-1003, ¶[78].

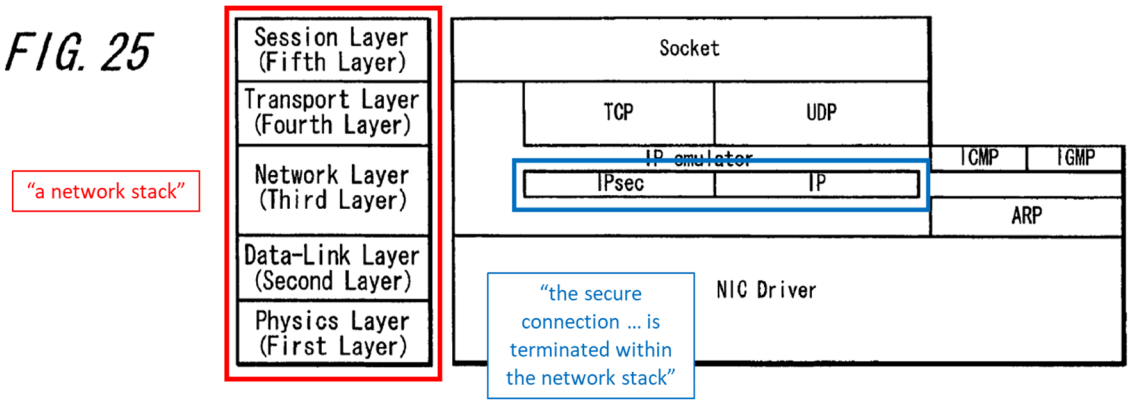
[12]

Houghton discloses that the push client "initiates an [sic] attempts to log into the push server 401 over data network 403" ("***the device messaging agent on at least one of the devices further to initiate the secure connection to the network message server***"). SAMSUNG-1005, 25:4-18. Indeed, Houghton claims such operation. SAMSUNG-1005, Claim 1 ("the push client initiates and maintains … a packet-based data connection … to the push server using Internet technologies"). SAMSUNG-1003, ¶[79].

[13]

As an initial matter, Dr. Traynor explains that a POSITA would have recognized or found obvious that connections between a server and a client would have been "***terminated within the network stack***" because this was well known in the art by the Critical Date (e.g., as in an HTTPS or IPsec connection, described

above). SAMSUNG-1003, ¶[80]; *see supra* [1.2], [4]-[5]. Indeed, Ozaki corroborates Dr. Traynor's testimony and discloses that IP and SSL protocols (e.g., IPsec) are contained within the "***network stack.***" SAMSUNG-1026, 3:40-60, FIGS. 25-26. Accordingly, the "***at least one of the devices [would have] a network stack in communication with the device messaging agent***" as Houghton uses these protocols to send push messages. SAMSUNG-1005, 17:13-25, 19:14-17. Additionally, Dr. Traynor explains that the secure protocols used by Houghton are also "***terminated within the network stack***," as evidenced by Ozaki. SAMSUNG-1005, 19:14-17; SAMSUNG-1026, 3:40-60, FIGS. 25-26; *see supra* [1.2], [4]-[5]; SAMSUNG-1003, ¶[80]. Ozaki's FIG. 25, reproduced below, illustrates various IP protocols within the network layer.



SAMSUNG-1026, FIG. 25 (annotated).

B. [GROUND 1B] – Claims 2 and 16-18 are rendered obvious by Houghton, Kalibjian, and Munson

1. Overview of Munson

Munson discloses a method of "pushing contents to client devices." SAMSUNG-1007, Abstract. Munson discloses "group pushes" where content is buffered and sent to multiple devices simultaneously, "serializ[ing]" content such that a series of messages are delivered to a particular device simultaneously, and various message queuing policies. SAMSUNG-1007, 3:7-67, 4:1-56, FIGS. 1-5. Illustrated below is an example process according to Munson. SAMSUNG-1007, FIG. 4; SAMSUNG-1003, ¶[81].

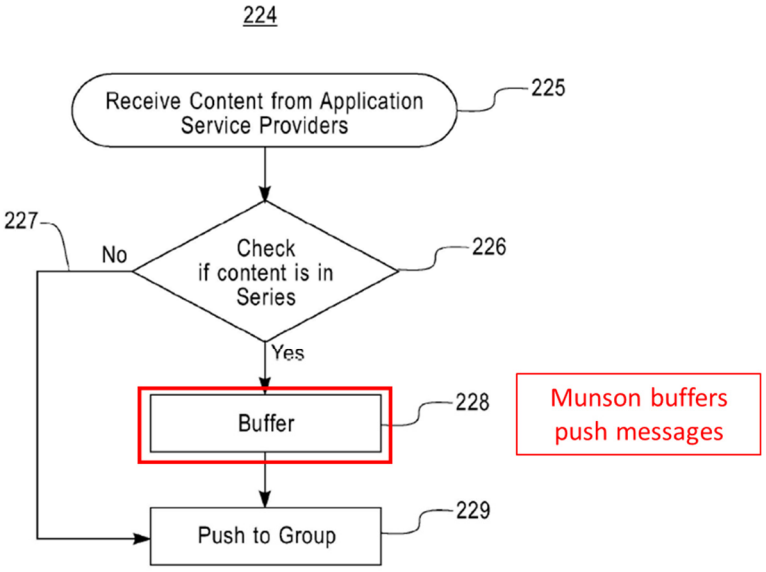


FIG. 4

SAMSUNG-1007, FIG. 4 (annotated).

2. Combination of Houghton-Kalibjian and Munson

It would have been obvious to a POSITA to combine the teachings of Houghton, Kalibjian, and Munson such that Houghton's system would collect and buffer messages. SAMSUNG-1003, ¶[82]. As one example, Munson's techniques of "group" pushes would have been incorporated into Houghton's system. SAMSUNG-1003, ¶[82]; *see supra* §§III.A.1, III.A.2, III.B.1. As Dr. Traynor explains, a POSITA would have combined Houghton, Kalibjian, and Munson to further improve service to the end user. SAMSUNG-1003, ¶[82].

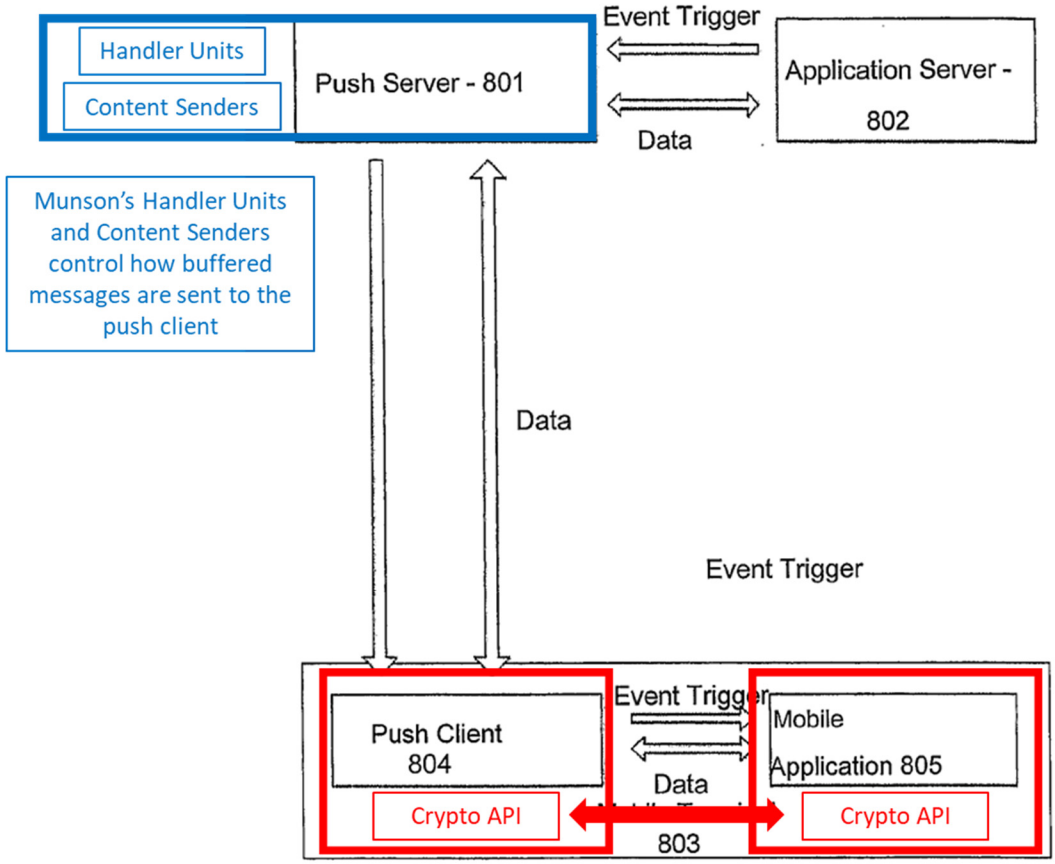
For instance, a POSITA would have recognized or found obvious that messages would need to be buffered when a mobile terminal does not have network connectivity. SAMSUNG-1003, ¶[83]. Indeed, Houghton recognizes this need. SAMSUNG-1005, 3:22-33 ("store and forward messaging systems"). Munson provides a conventional software-capable solution that would have been efficient to implement within the existing hardware of Houghton's system. SAMSUNG-1005, 3:22-33, FIGS. 3-4; SAMSUNG-1007, 3:40-67, 4:1-42, FIG. 3; SAMSUNG-1003, ¶[83].

As explained below in more detail, combining Houghton, Kalibjian, and Munson would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to

yield predictable results and (2) the use of known technique to improve similar devices (methods, or products) in the same way. *See KSR,* 550 U.S. at 415-421; MPEP §2143; SAMSUNG-1003, ¶[84].

Incorporating Munson's method of buffering and pushing messages into Houghton's push message system would also have been predictable and foreseeable with a reasonable expectation of success because Houghton already discloses such methods. SAMSUNG-1005, 3:22-33, FIGS. 3-4; SAMSUNG-1003, ¶[85]. Additionally, Munson, like Houghton and Kalibjian, discloses that its methods can be implemented for "mobile users" (consistent with the mobile terminals described by Houghton). SAMSUNG-1005, 16:16-36, 17:1-2; SAMSUNG-1006, ¶[0011]; SAMSUNG-1007, 1:11-26; SAMSUNG-1003, ¶[85].

In the combined Houghton-Kalibjian-Munson system, illustrated below in Houghton's Figure 8, Munson's handler units and content senders would have been incorporated into Houghton's push server such that they would buffer and push messages based on the policies described by Munson. SAMSUNG-1005, 3:22-33, FIGS. 3-4; SAMSUNG-1007, 3:40-67, 4:1-42, FIG. 3; SAMSUNG-1003, ¶[86].



SAMSUNG-1005, FIG. 8 (modified to incorporate Kalibjian and Munson).

3. Analysis

[2]

As Dr. Traynor explains, the Houghton-Kalibjian-Munson combination renders this claim obvious in multiple ways. SAMSUNG-1003, ¶[87].

First, Houghton discloses the "SMS (Short Message Service)" and "MMS (Multi-media Messaging Service)" that "store and forward" messages ("***collect and buffer multiple requests to transmit application data***"). SAMSUNG-1005, 3:22-33, FIGS. 3-4; SAMSUNG-1003, ¶[88].

Second, consistent with the disclosure of Houghton, Munson discloses a "Series Handler Unit 224" that "receives contents from application service providers" and uses a "series buffer … to keep the contents until all contents in a series arrive" ("***collect and buffer multiple requests to transmit application data***"). SAMSUNG-1007, 3:66-67, 4:1-11. Munson's Figure 3 illustrates a structure for queuing messages in a content push service 220. SAMSUNG-1007, FIG. 3; SAMSUNG-1003, ¶[89].

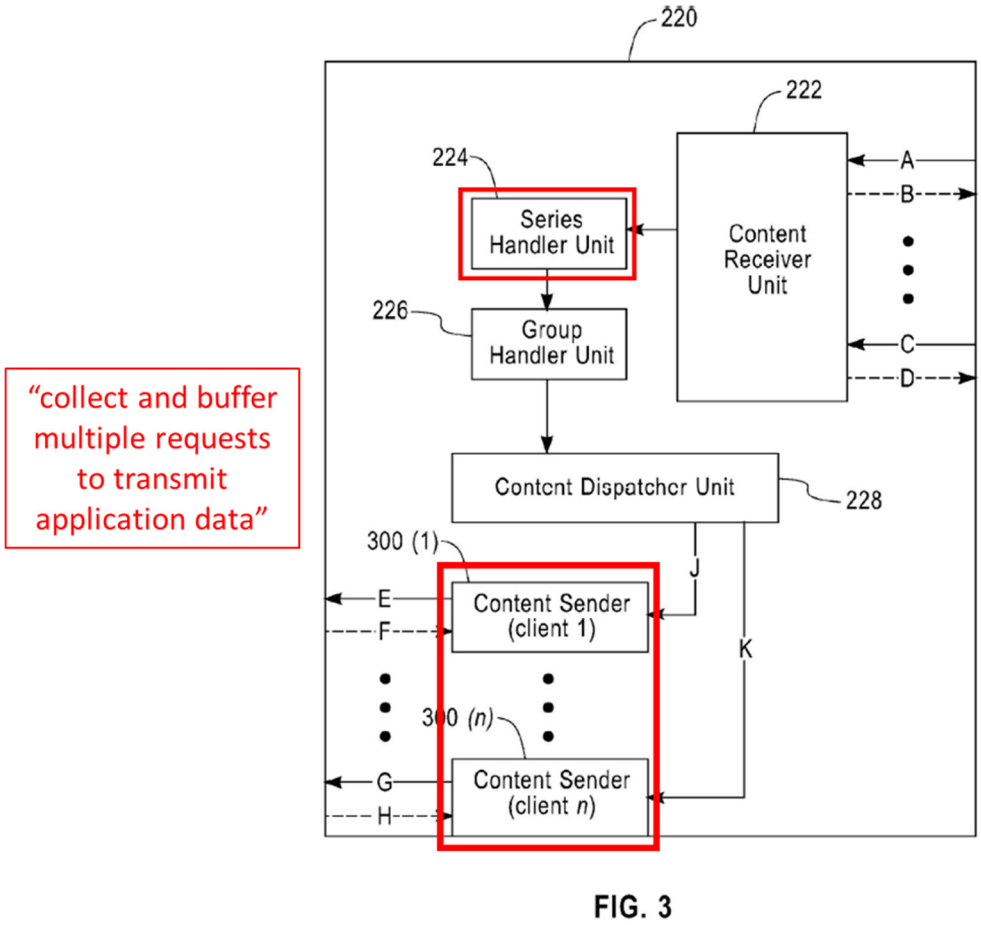
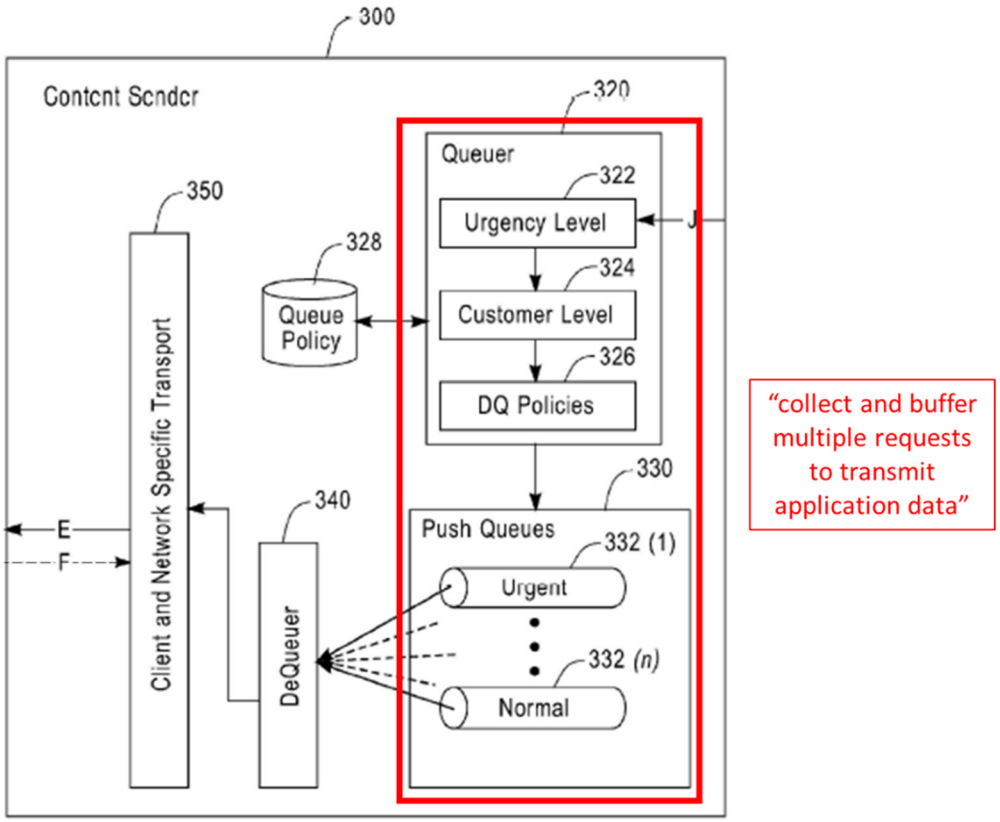


FIG. 3

SAMSUNG-1007, FIG. 3 (annotated).

Third, Munson discloses a plurality of "Content Sender[s] 300" that each contain a "Queuer 320" and "Push Queues 330" ("***collect and buffer multiple requests to transmit application data***"). SAMSUNG-1007, 4:12-42, FIGS. 3, 5. Munson discloses that when pushing messages, content senders 300 check "urgency level of contents … customer level … [and] dequeue policy." *Id.* Moreover, each "client device" (e.g., the Houghton-Kalibjian-Munson mobile terminal) is assigned a content sender 300 ("***a particular one of the devices***"). *Id.*, 3:40-65. Munson's Figure 5 illustrates a structure for queuing messages in a content sender 300. SAMSUNG-1007, FIG. 5; SAMSUNG-1003, ¶[90].



SAMSUNG-1007, FIG. 5 (annotated).

[16]

As Dr. Traynor explains, the Houghton-Kalibjian-Munson combination renders this claim obvious in multiple ways. SAMSUNG-1003, ¶[91].

First, Munson discloses that "content can be pushed according to a schedule of time or event" ("***a transmission trigger***") and provides an example where a "group push" is performed "during off-peak hours to take advantage of lower rates." SAMSUNG-1007, 5:32-36; SAMSUNG-1003, ¶[92].

Second, Houghton discloses that a "periodic message" ("***a transmission trigger***") is sent from the server to the client such that "client socket, server socket, intermediate Network Address Translation (NAT) devices, intermediate firewalls, and intermediate gateway devices do not time expire the connection." SAMSUNG-1005, 19:18-21; SAMSUNG-1003, ¶[93].

[17]

As described above in [16], both Houghton and Munson describe that a "***periodic timer***" is used as a "***transmission trigger***." SAMSUNG-1005, 19:18-21; SAMSUNG-1007, 5:32-36; *see supra* [16]; SAMSUNG-1003, ¶[94].

[18]

Houghton discloses that "the push client 405 may monitor the local resources for a state change (a trigger event)" and "send a message to the server 401" ("***a transmission from the device messaging agent of the particular device***").

SAMSUNG-1005, 26:32-35. As Dr. Traynor explains, a POSITA would have recognized or found obvious that communication from a mobile terminal (e.g., the device messaging agent) would have been used as a trigger to transmit buffered messages as this communication is an indicator of the mobile terminal entering an area of network connectivity. SAMSUNG-1003, ¶[95]; *see supra* [16].

C. [GROUND 1C] – Claims 14-15 are rendered obvious by Houghton, Kalibjian, and Rakic

1. Overview of Rakic

Rakic discloses a mobile device that "receive[s] a secure push message from an administrator device" where the device "validate[s] the secure push message based on the electronic signature." SAMSUNG-1008, Abstract, ¶¶[0041]-[0050], [0069], FIG. 1. Rakic's electronic signatures are created by "generat[ing] a first key by combining an administrator code, a client device identifier that identifies a client device, and subscriber information that is associated with a service to which a user subscribes." *Id*. The device then "hash[es] the first key to generate a second key, and use[s] the second key to sign a data block within the secure push message to produce an electronic signature." *Id*. Rakic additionally discloses a "database device 108" that contains information regarding "electronic signatures" used to "authenticate the sender" of a message. SAMSUNG-1008, ¶¶[0041]-[0050]; SAMSUNG-1003, ¶[96]. An overview of Rakic's system is presented below.

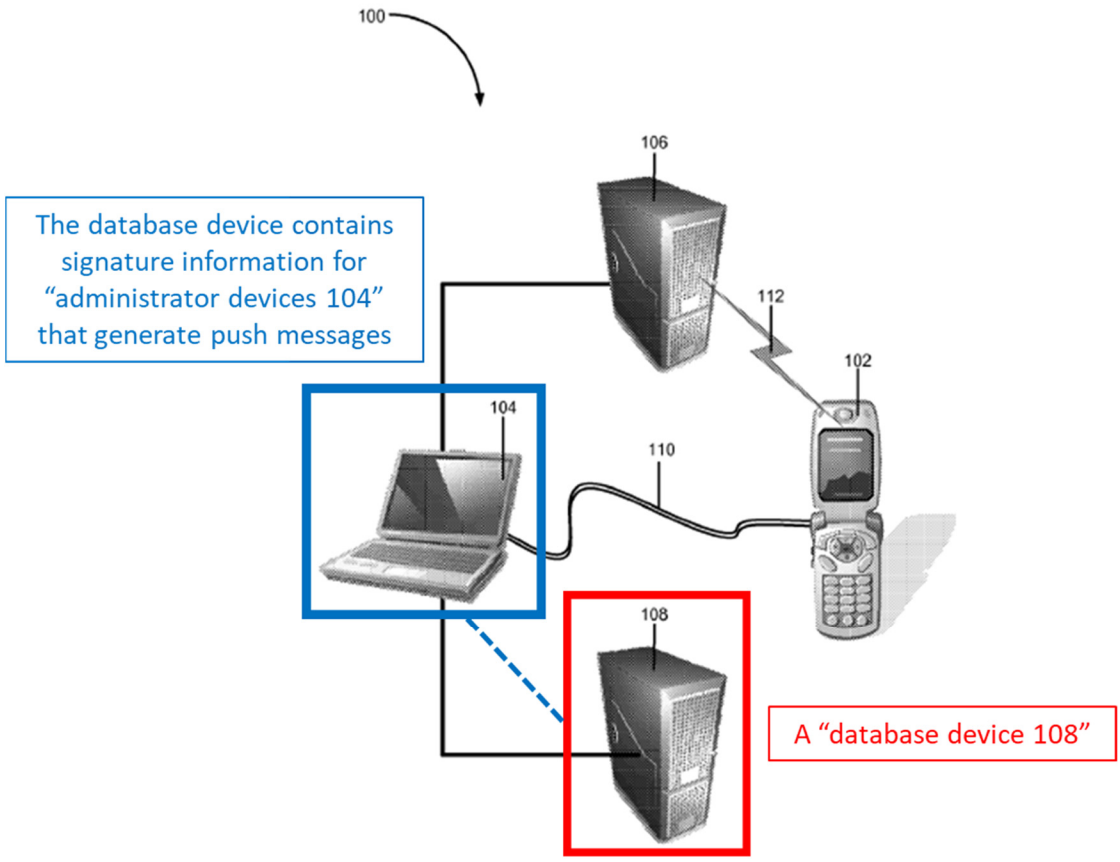


Fig. 1

SAMSUNG-1008, FIG. 1 (annotated).

2. Combination of Houghton-Kalibjian and Rakic

It would have been obvious to a POSITA to combine the teachings of Houghton, Kalibjian, and Rakic to add authentication services to Houghton's system. SAMSUNG-1003, ¶[97]. As one example, Rakic's database device and authentication methods would have been incorporated into the push message system of Houghton. SAMSUNG-1005, 23:3-21; SAMSUNG-1008, ¶¶[0041]-[0050], [0069]; SAMSUNG-1003, ¶[97]; *see supra* §§III.A.1, III.A.2, III.C.1. As Dr.

Traynor explains, a POSITA would have combined Houghton, Kalibjian, and Rakic to further improve the security of the system. SAMSUNG-1003, ¶[97].

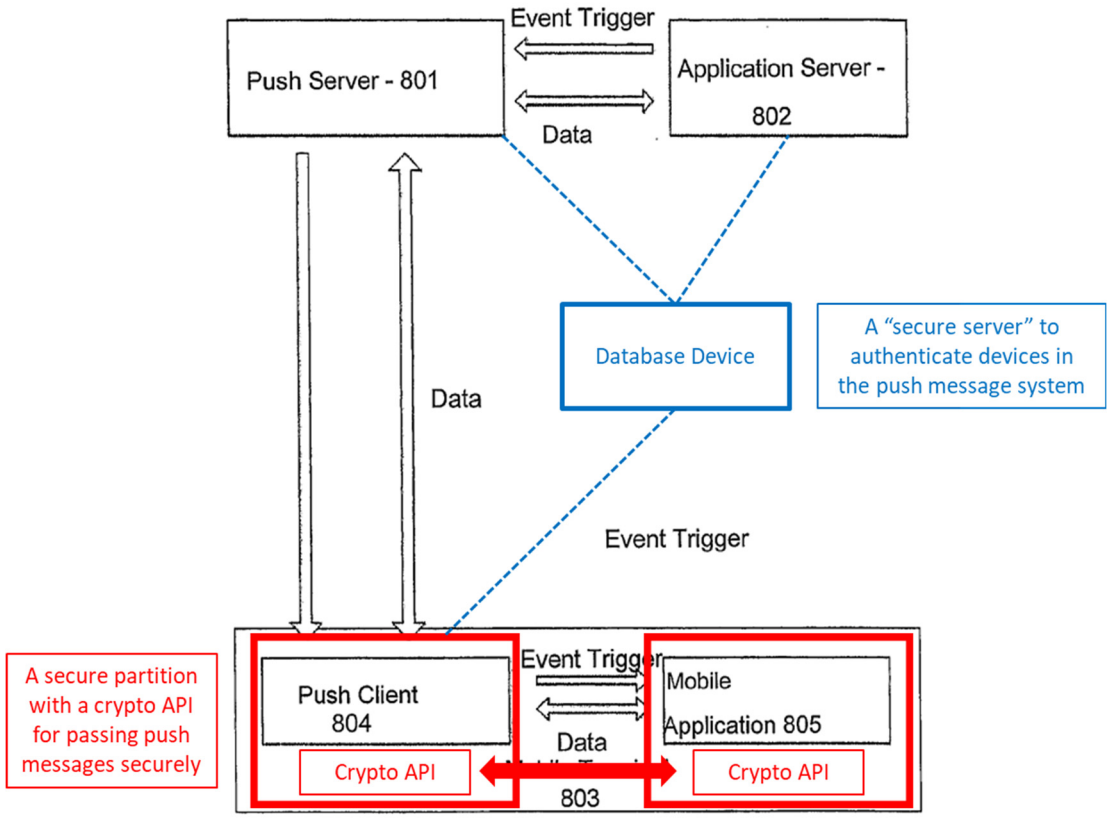
For instance, a POSITA would have recognized that Rakic's authentication methods would have improved the security of Houghton's push message system when such a system is scaled up to encompass many application servers and mobile terminals across a global network (i.e., thousands of different devices). SAMSUNG-1005, 23:3-21; SAMSUNG-1008, ¶¶[0041]-[0050], [0069]; SAMSUNG-1003, ¶[98].

As explained below in more detail, combining Houghton, Kalibjian, and Rakic would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results and (2) the use of known technique to improve similar devices (methods, or products) in the same way. *See KSR,* 550 U.S. at 415-421; MPEP §2143; SAMSUNG-1003, ¶[99].

Incorporating Rakic's database device and authentication methods into Houghton's push message system would also have been predictable and foreseeable with a reasonable expectation of success because Houghton already discloses implementing security measures in its push message system. SAMSUNG-1005, 23:3-21; SAMSUNG-1003, ¶[100]. Additionally, Rakic, like Houghton and Kalibjian, discloses that its methods can be implemented for "mobile telephone[s]"

(consistent with the mobile terminals described by Houghton). SAMSUNG-1005, 16:16-36, 17:1-2; SAMSUNG-1006, ¶[0011]; SAMSUNG-1008, ¶[0044]; SAMSUNG-1003, ¶[100].

In an example of the combined Houghton-Kalibjian-Rakic system, illustrated below in Houghton's Figure 8, Rakic's database device and authentication methods would have been incorporated into Houghton's push message system such that devices that use the system (e.g., an application server or push client) would have been authenticated prior to sending messages. SAMSUNG-1005, 23:3-21; SAMSUNG-1008, ¶¶[0041]-[0050], [0069]; SAMSUNG-1003, ¶[101].



SAMSUNG-1005, FIG. 8 (modified to incorporate Kalibjian and Munson).

3. Analysis

[14]

Rakic discloses a configuration process where the "administrator device 104 … obtain[s] information that is specific to client device 102, store[s] the information in a database on database device 108, and store[s] an administrator code in client device 102." SAMSUNG-1008, ¶[0048]. Once this information is obtained, the "administrator device 104 … retrieve[s] the information related to client device 102 from database device 108, [and] generate[s] an electronic signature by signing a message based on the information." SAMSUNG-1008, ¶[0049]; SAMSUNG-1003, ¶[102].

As Dr. Traynor explains, a POSITA would have recognized or found obvious that, in the above process, "***at least one of the applications on at least one of the devices and the network application server corresponding to that application authenticate with each other prior to passing application data via the device messaging agent on that device and the network message server***" because Rakic's configuration process obtains information used to generate signatures needed for message passing. SAMSUNG-1008, ¶[0041]-[0051]; SAMSUNG-1003, ¶[103].

Moreover, Dr. Traynor explains that authentication between servers and applications was well known in the art as of the Critical Date. SAMSUNG-1003,

¶[104]. For example, Shenfield, a European patent directed to a "[p]ush framework for delivery of dynamic mobile content," describes a "push proxy 410" that "can check whether the application is … registered to obtain content from a content provider 110" (e.g., whether the application has authenticated with the content provider) prior to sending "content" and "notification[s]." SAMSUNG-1014, ¶¶[0143]-[0165]; SAMSUNG-1003, ¶[104].

[15]

As an initial matter, the '117 Patent does not define a "secure server" or "secure authorization list," but discusses "agent level access authorization, which only allows access to the agents that are on the secure authorization list and in which the list is provided by the secure server and signatures are provided by the secure server." SAMSUNG-1001, 42:31-35. While the above disclosure does not recite the features of the claim,[8] Petitioner has used these statements to guide the below analysis in the absence of any comprehensive disclosure of the claim features in the '117 Patent. SAMSUNG-1003, ¶[105].

Rakic discloses a "database device 108" ("***secure server***") that contains information regarding "electronic signatures" used to "authenticate the sender" of a

[8] Petitioner reserves the right to raise clarity and written description support arguments in co-pending litigation.

message ("***a secure authorization list, the secure authorization list indicating the applications and network application servers that are allowed to communicate using the network message server***"). SAMSUNG-1008, ¶¶[0041]-[0050], [0069]. As Dr. Traynor explains, authentication servers, like Rakic's "database device 108" were well known in the art by the Critical Date. SAMSUNG-1003, ¶[106]. Indeed, Monjas-Llorente corroborates Dr. Traynor's testimony and discloses a "AAA (Authentication, Authorization, and Accounting) server" that "authenticates users, authorizes services for the users when the users access the network." SAMSUNG-1017, Abstract, ¶[0002]. As Dr. Traynor explains, "AAA services, like those described in Rakic, were (and still are) commonly used to maintain lists of devices, services, and applications that are authorized to use a particular network and the incorporation of AAA services into Houghton's push message system (e.g., Rakic's database device) would have been well within the general knowledge and capability of a POSITA." SAMSUNG-1003, ¶[106].

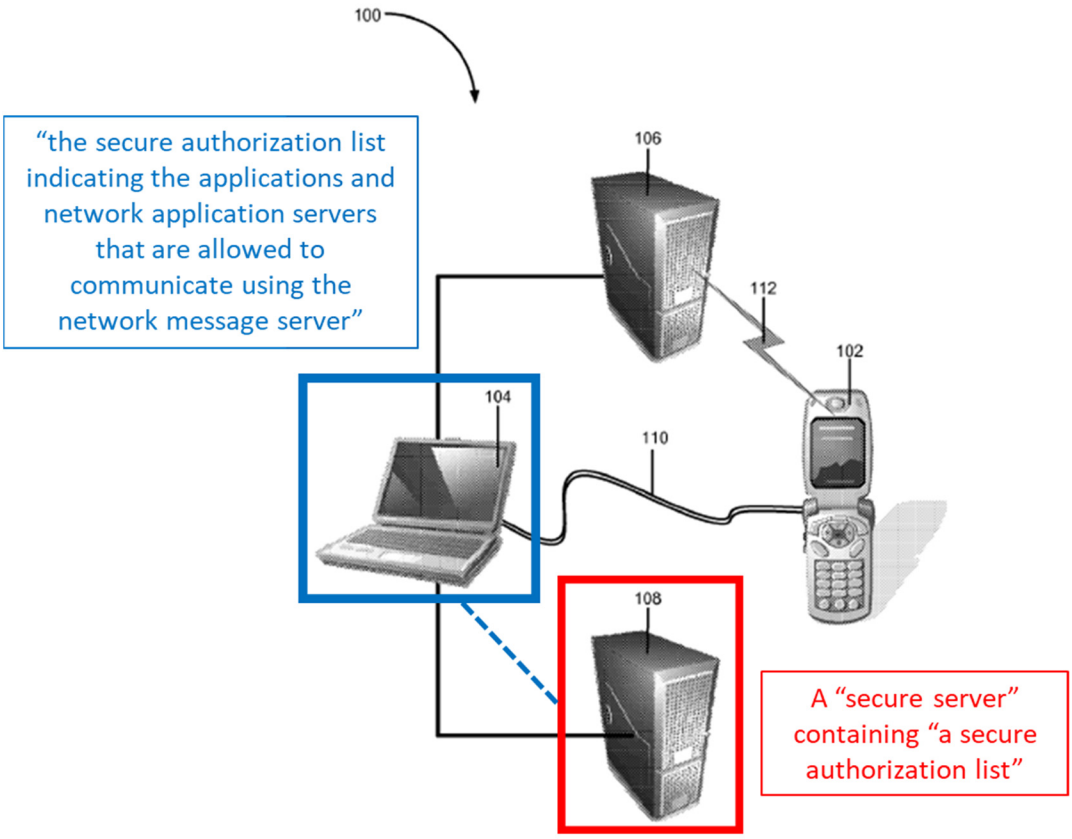


Fig. 1

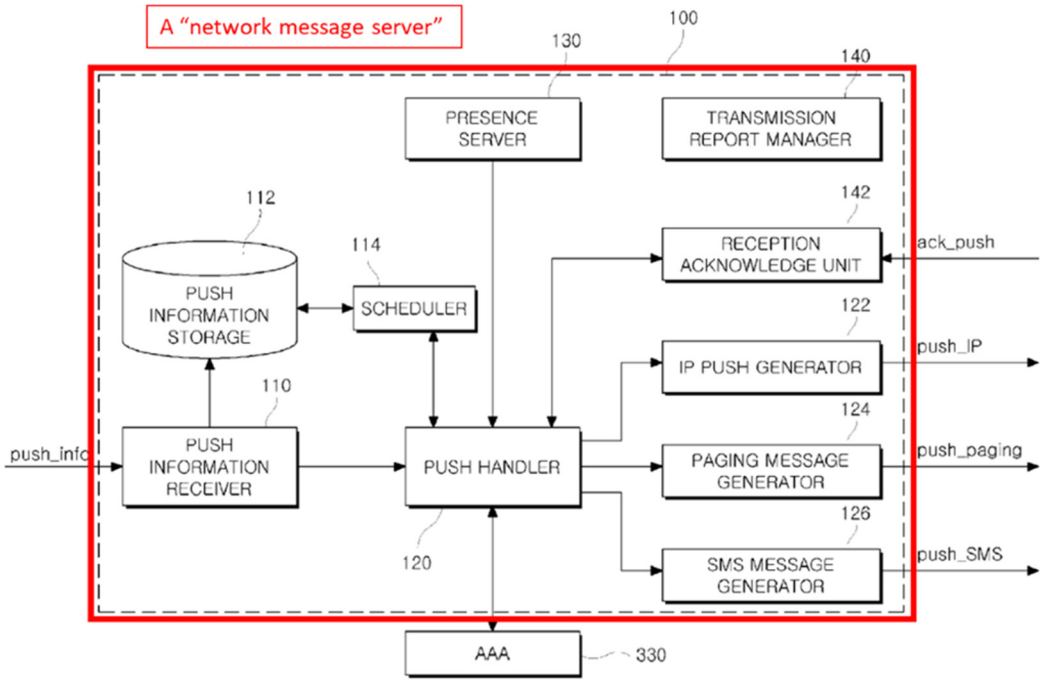
SAMSUNG-1008, FIG. 1 (annotated).

D. [GROUND 2A] – Claims 1, 3-6, 9-11, and 13-15 are rendered obvious by Lee, Ellison, and Anderson

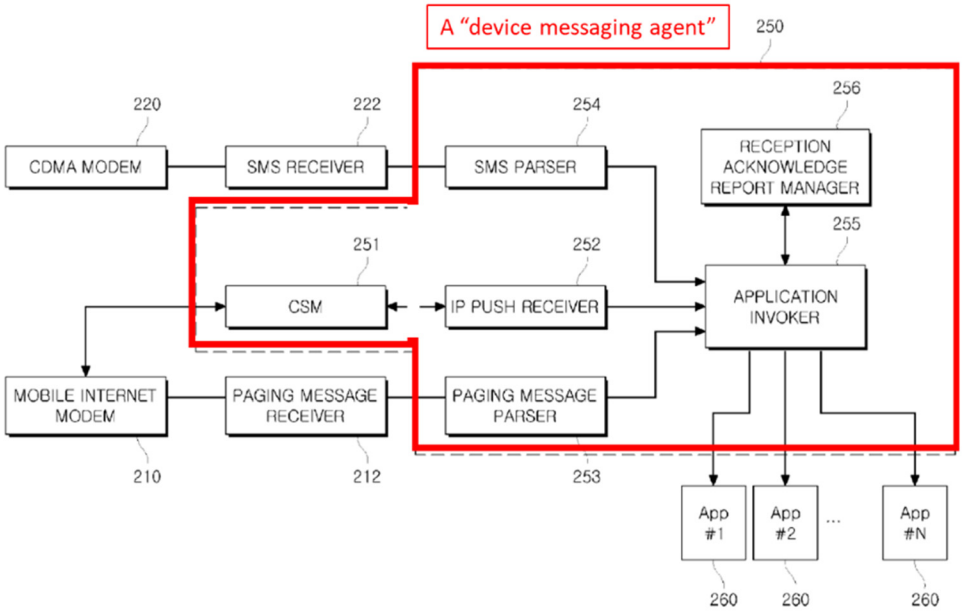
1. Overview of Lee

Lee discloses "a system and a method for providing an integrated push service in an internet service network." SAMSUNG-1012, Abstract. This system includes "a plurality of push application servers for providing … push information," which further includes "push data invoked through an application of a mobile terminal." *Id*. Lee's mobile terminals include "a communication session manager

resident in a memory," which maintains "a communication session with the integrated push service server." *Id.*; SAMSUNG-1003, ¶[107].



SAMSUNG-1012, FIG. 2 (annotated).



SAMSUNG-1012, FIG. 4 (annotated).

2. Overview of Ellison

Ellison discloses a "method and apparatus to protect a subset of a software environment." SAMSUNG-1013, Abstract. This includes a plurality of "operating system nub key[s] (OSNK)," which are "unique to an operating system (OS) nub." *Id*. A "usage protector" uses the OSNK to "protect usage of [a] subset of the software environment." *Id*.; SAMSUNG-1003, ¶[108].

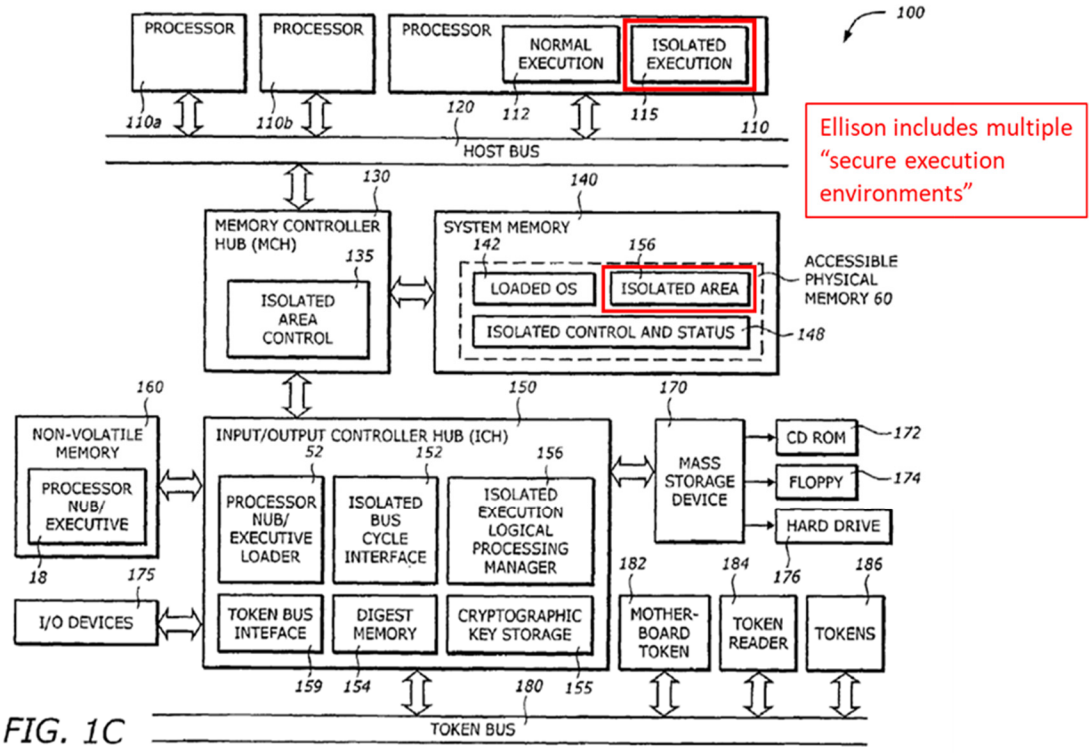


FIG. 1C

SAMSUNG-1013, FIG. 1C (annotated).

3. Overview of Anderson

Anderson is a textbook entitled "Security Engineering" written by Ross Anderson, a Professor in Security Engineering at Cambridge University who is "[w]idely recognized as one of the world's foremost authorities on security."

SAMSUNG-1010, p. 3. Anderson describes security solutions on many platforms to include "Telecom system[s]." *Id*., pp. 9, 21, 26-63. Anderson also describes various examples of secure internet protocols. *Id*., pp. 64-109; SAMSUNG-1003, ¶[109].

4. Combination of Lee and Ellison

It would have been obvious to a POSITA to combine the teachings of Lee and Ellison and employ secure interprocess communication in Lee's devices. SAMSUNG-1003, ¶[110]. As one example, Ellison's secure platform would have been incorporated into the mobile terminals of Lee. SAMSUNG-1012, ¶¶[22]-[29], FIGS. 1-2; SAMSUNG-1013, 8:25-32, 8:66-67, 9:1-6, 9:28-62, FIG. 2; SAMSUNG-1003, ¶[110]. As Dr. Traynor explains, a POSITA would have combined Lee and Ellison to improve the security of Lee's mobile terminal. SAMSUNG-1003, ¶¶[110]-[113]. For instance:

1) A POSITA would have recognized that Ellison's secure platform would have improved the security of Houghton's push message system by improving device security (i.e., entry points to the network). SAMSUNG-1012, ¶¶[22]-[29], FIGS. 1-2; SAMSUNG-1013, 8:25-32, 8:66-67, 9:1-6, 9:28-62, FIG. 2.; SAMSUNG-1003, ¶[111].

2) As Dr. Traynor explains, the increased confidence in device and/or net-

work security provided by Ellison would have enabled a POSITA to expand the Lee push service to additional application servers and clients. SAMSUNG-1012, ¶¶[22]-[29], FIGS. 1-2; SAMSUNG-1013, 8:25-32, 8:66-67, 9:1-6, 9:28-62, FIG. 2.; SAMSUNG-1003, ¶[112].

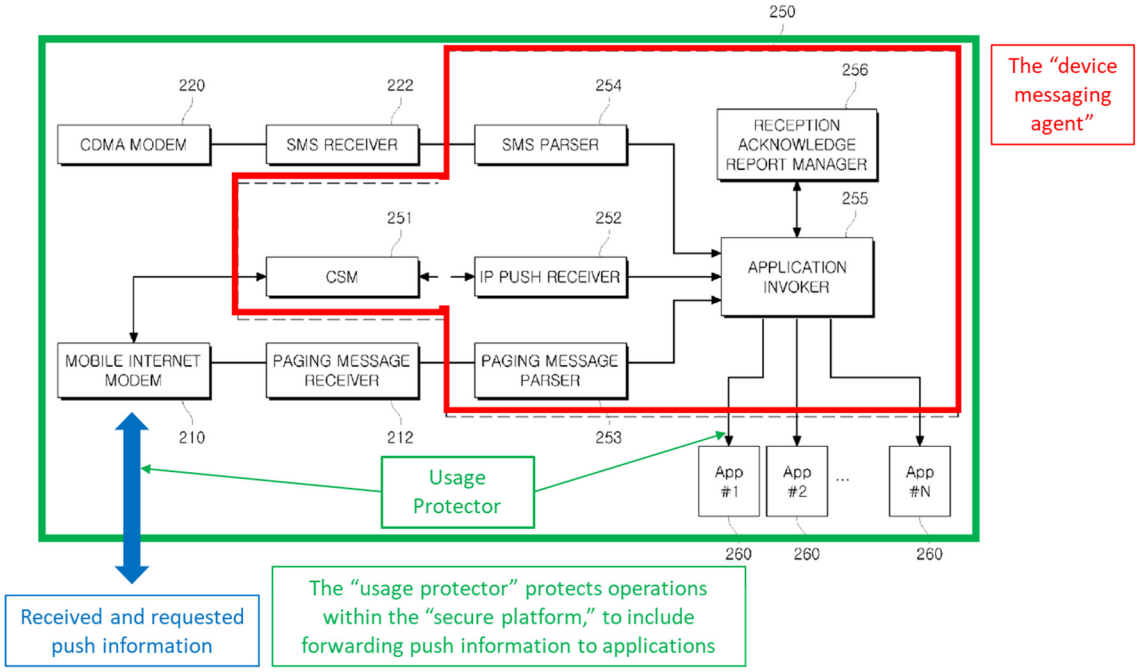
3) Dr. Traynor also explains that "device level security improvements are an efficient, low-cost option for improving network security, which would have been a natural solution for the Lee system which is concerned with 'the cost for building the network.'" SAMSUNG-1012, ¶[2]; SAMSUNG-1013, 8:25-32, 8:66-67, 9:1-6, 9:28-62, FIG. 2.; SAMSUNG-1003, ¶[113].

As explained below in more detail, combining Lee and Ellison would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results. *See KSR,* 550 U.S. at 415-421; MPEP §2143; SAMSUNG-1003, ¶[114].

Incorporating Ellison's security techniques into Lee's mobile terminals would also have been predictable and foreseeable with a reasonable expectation of success because Ellison describes that its techniques can be implemented in "computer system[s]" that contain a "processor." SAMSUNG-1013, 5:11-16; SAMSUNG-1003, ¶[115]. A POSITA would have recognized or found obvious that the examples of "mobile terminals" provided in Lee would have contained at least one

"processor" capable of implementing Ellison's techniques because it was known in the art that mobile terminals contained processors. SAMSUNG-1012, ¶¶[22]-[29], FIG. 1; SAMSUNG-1003, ¶[115].

In the combined Lee-Ellison system, illustrated below in Lee's Figure 2, Ellison's secure platform would have been incorporated into Lee's mobile terminals. SAMSUNG-1012, ¶¶[22]-[29], FIGS. 1-2; SAMSUNG-1013, 8:25-32, 8:66-67, 9:1-6, 9:28-62, FIG. 2; SAMSUNG-1003, ¶[116].



SAMSUNG-1012, FIG. 2 (modified to incorporate Ellison).

5. Combination of Lee-Ellison and Anderson

It would have been obvious to a POSITA to combine the teachings of Lee, Ellison, and Anderson to use secure communication protocols. SAMSUNG-1003,

¶[117]. As one example, Anderson's secure internet protocols would have been incorporated into the network system of Lee-Ellison. SAMSUNG-1012, ¶¶[22]-[29], FIGS. 1-2; SAMSUNG-1010, pp. 64-109; SAMSUNG-1003, ¶[117]. As Dr. Traynor explains, a POSITA would have combined Lee, Ellison, and Anderson to improve the security of Lee-Ellison's network system. SAMSUNG-1003, ¶¶[117]-[119]. For instance:

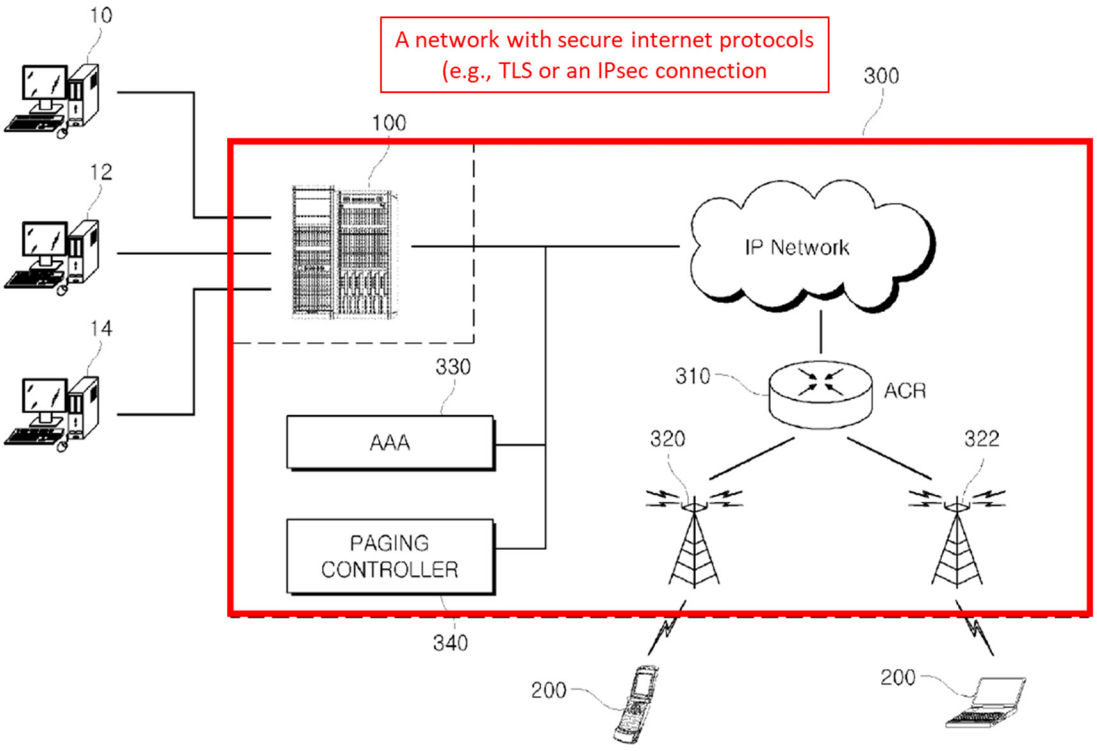
1) As Dr. Traynor explains, a POSITA would have "naturally sought to implement basic secure protocols in Lee's network system that were well within their knowledge." SAMSUNG-1012, ¶¶[22]-[29], FIGS. 1-2; SAMSUNG-1010, pp. 64-109; SAMSUNG-1003, ¶[118]. Indeed, Dr. Traynor explains that "if a POSITA decided to build a network system without such security measures, the operating costs would have been extreme, especially for a mobile push system serving potentially thousands of clients and servers. Unsecure networks are easily compromised, which leads to significant down-time and financial burden on the operator." SAMSUNG-1012, ¶[2]; SAMSUNG-1003, ¶[118].
2) Anderson discloses that security vulnerabilities can be widespread in mobile networks. SAMSUNG-1010, pp. 37-63. As discussed above, a POSITA would have recognized their financial exposure to such vulnerabilities and implemented Anderson's teachings to minimize this risk.

SAMSUNG-1010, pp. 64-109; SAMSUNG-1003, ¶[119].

As explained below in more detail, combining Lee, Ellison, and Anderson would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results. *See KSR,* 550 U.S. at 415-421; MPEP §2143; SAMSUNG-1003, ¶[120].

Incorporating Anderson's secure internet protocols into Lee-Ellison's network system would also have been predictable and foreseeable with a reasonable expectation of success because Anderson, like Lee, describes that its techniques can be implemented in "Telecom system[s]." SAMSUNG-1010, pp. 9, 21, 26-63; SAMSUNG-1003, ¶[121].

In the combined Lee-Ellison-Anderson system, illustrated below in Lee's Figure 1, Anderson's secure internet protocols would have been incorporated into Lee's network system. SAMSUNG-1012, ¶¶[22]-[29], FIGS. 1-2; SAMSUNG-1010, pp. 64-109; SAMSUNG-1003, ¶[122].

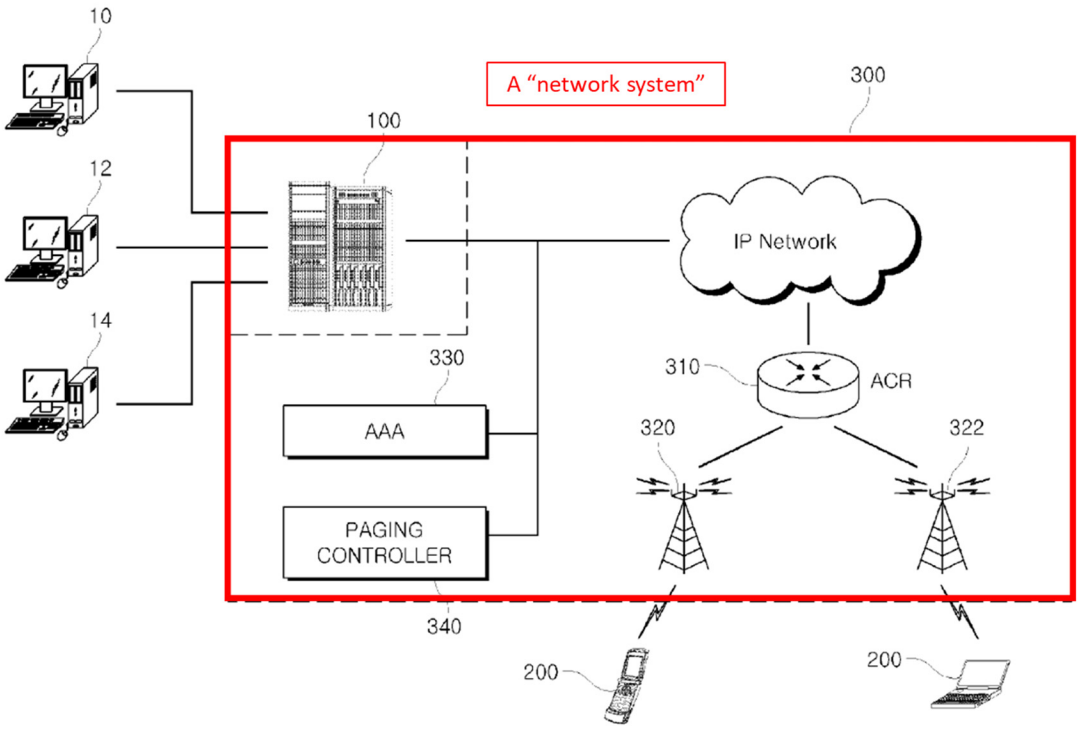


SAMSUNG-1012, FIG. 1 (modified to incorporate Ellison and Anderson).

6. Analysis

[1.pre]

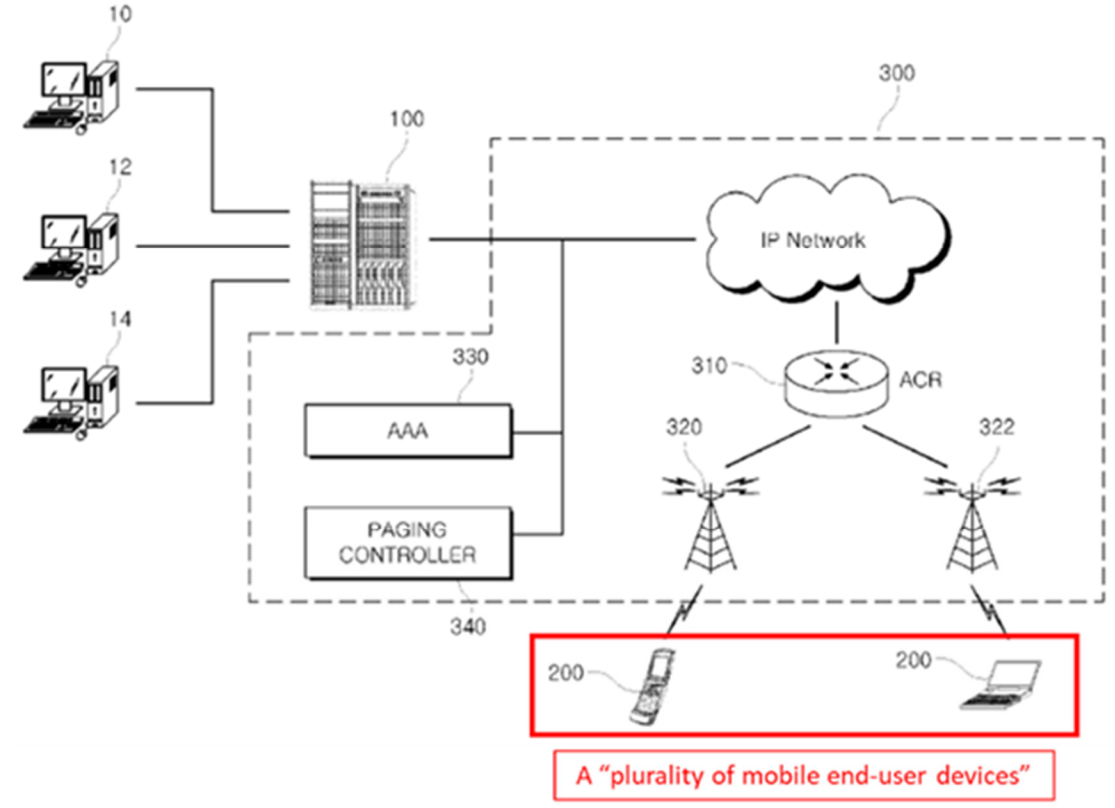
To the extent the preamble is limiting, Lee teaches or renders it obvious. Lee discloses "a system and a method for providing an integrated push service in an internet service network" ("***[a] network system***"). SAMSUNG-1012, Abstract, ¶¶[22], [25]-[27], FIGS. 1-3; SAMSUNG-1003, ¶[123].



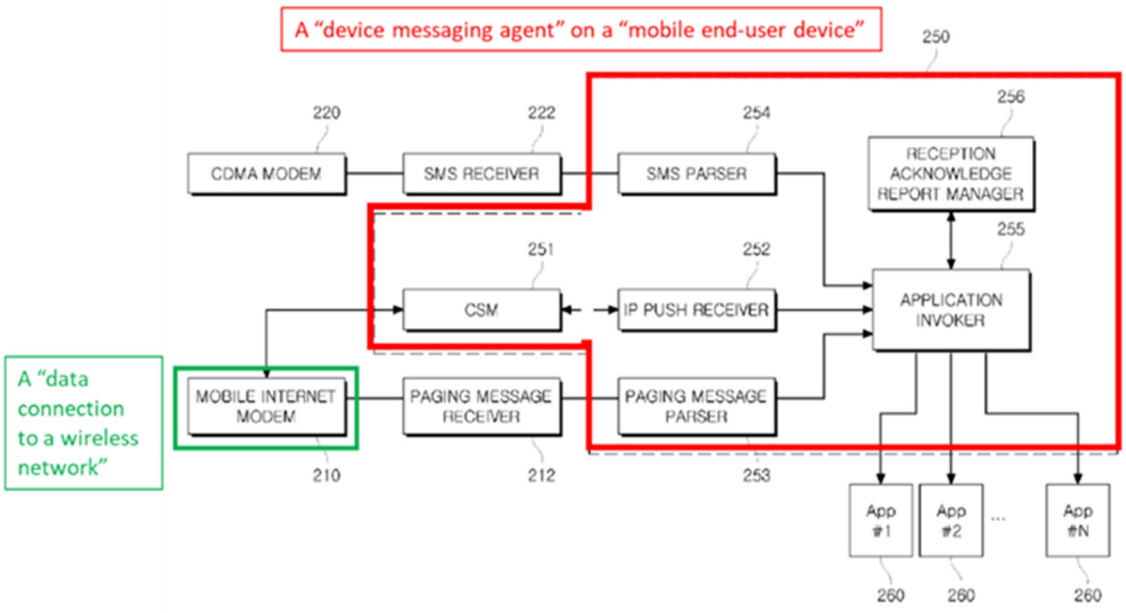
SAMSUNG-1012, FIG. 1 (annotated).

[1.1]

Lee discloses a "push service agent 250" ("***device messaging agent***") operating on "mobile terminal 200" ("***executable on a respective one of a plurality of mobile end-user devices***") that "maintains [a] communication session with the integrated push service server 100" ("***configured to exchange Internet data via a data connection to a wireless network***") and "selectively invokes the application 260 … of the push information … to deliver the push data." SAMSUNG-1012, ¶¶[25], [28]-[29], [34], [44], [49]-[52], FIGS. 1, 4; SAMSUNG-1003, ¶[124]. As shown in Figure 1, Lee's system has a "***plurality***" of mobile devices 200 and push service agents 250. SAMSUNG-1012, FIG. 1; *see id.*, FIG. 4.



SAMSUNG-1012, FIG. 1 (annotated).

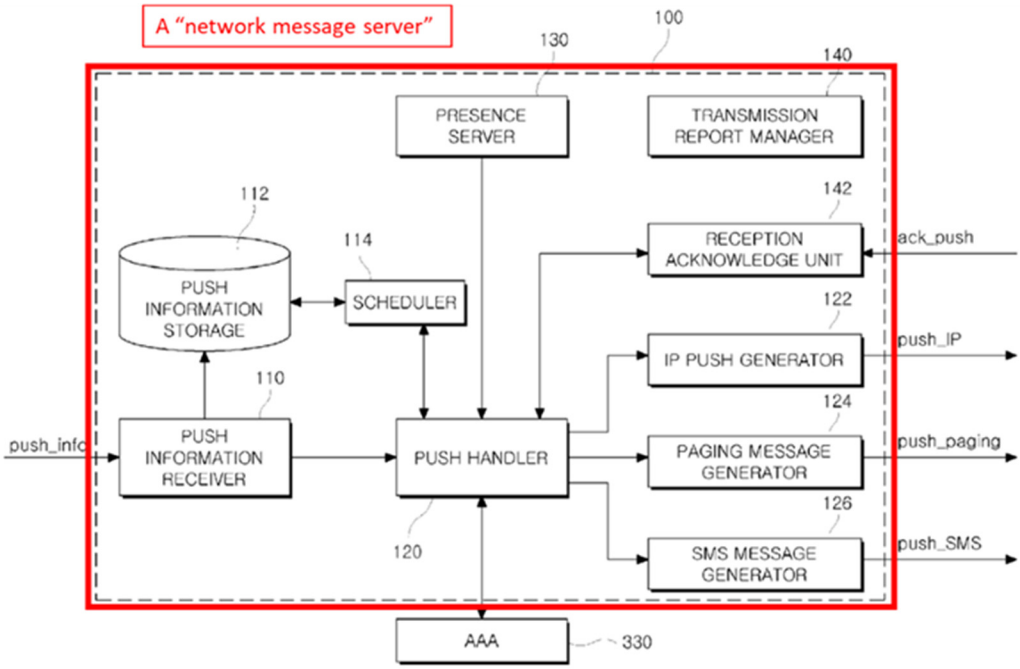


SAMSUNG-1012, FIG. 4 (annotated).

Moreover, "mere duplication of parts has no patentable significance unless a new and unexpected result is produced." *In re Harza*, 274 F.2d 669.

[1.2]

Lee discloses a "push service server 100" ("***a network message server***") that receives "push information" from a plurality of "application servers" and "provides the push information … to the mobile terminal 200." SAMSUNG-1012, ¶¶[22], [25]-[29], FIGS. 1-3; SAMSUNG-1003, ¶[125].



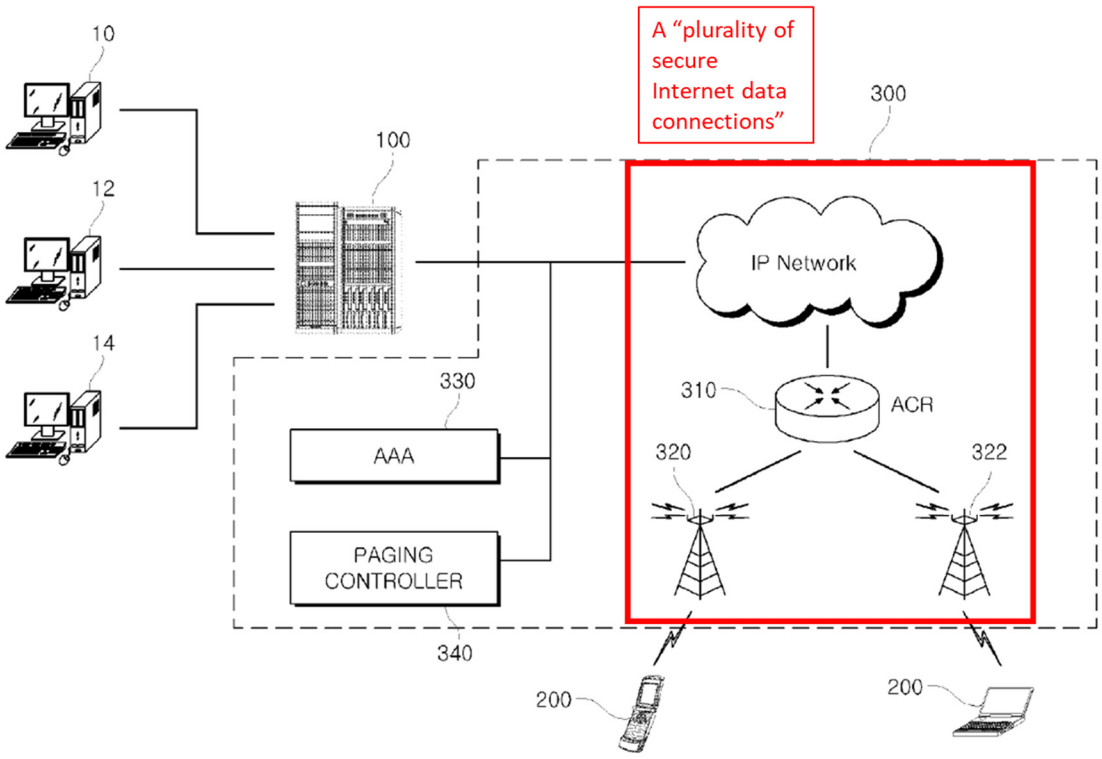
SAMSUNG-1012, FIG. 2 (annotated).

As described above, Lee's system has a "***plurality***" of mobile devices 200 and push service agents 250 in communication over a network. SAMSUNG-1012, FIGS. 1, 4; *see supra* [1.1]. Additionally, Lee discloses that this network is a "mobile internet network" ("***a plurality of … Internet data connections … between***

the network message server and … mobile end-user devices via a device data connection to a wireless network"). SAMSUNG-1012, ¶¶[13], [24]-[29]; SAMSUNG-1003, ¶[126].

As Dr. Traynor explains (and Anderson discloses), a POSITA would have recognized or found obvious that internet connections to a mobile device would have been made to be "***secure***[9]." SAMSUNG-1010, pp. 26-63; *see supra* §III.D.3. For example, Anderson discloses examples of secure internet protocols, including "IPsec" and Transport Layer Security ("TLS") that support encryption and authentication. SAMSUNG-1010, pp. 100-103; *see supra* §III.D.3. Secure internet protocols, as disclosed by Anderson, would have been incorporated into Lee's mobile internet network ("***a plurality of secure Internet data connections***"). SAMSUNG-1012, ¶¶[13], [24]-[29], FIG. 1; SAMSUNG-1010, pp. 100-103; *see supra* §§III.D.3, III.D.5; SAMSUNG-1003, ¶[127].

[9] While Anderson describes that security in mobile networks is far from perfect, it makes clear the distinction that security in these networks is of great importance. SAMSUNG-1010, pp. 26-63; SAMSUNG-1003, ¶[127].

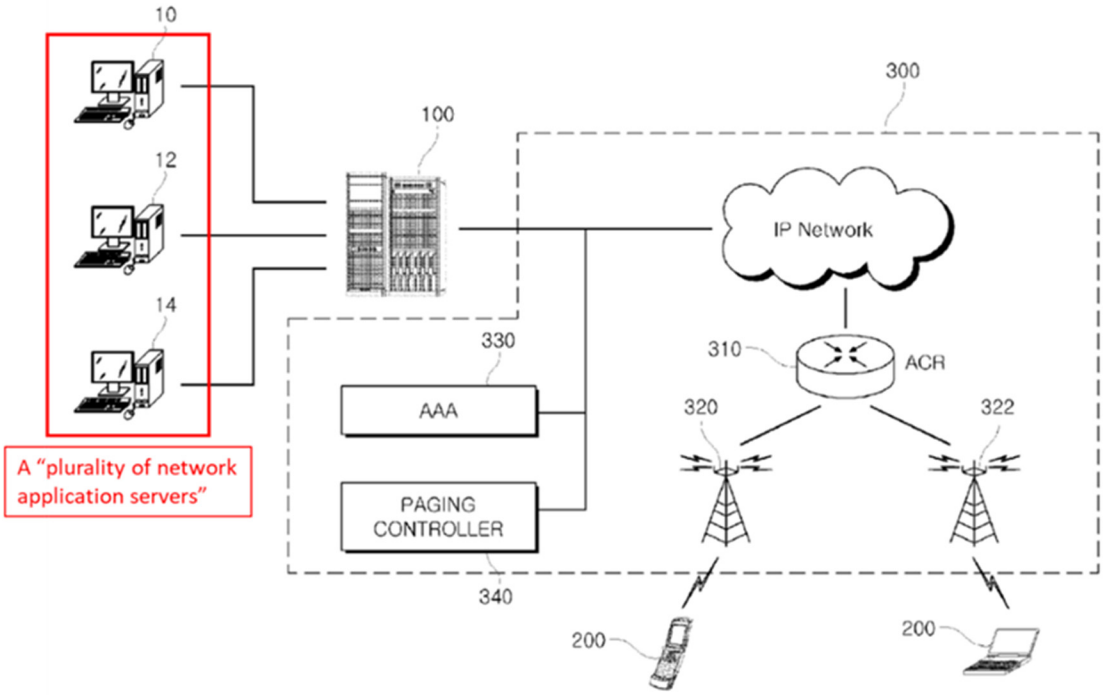


SAMSUNG-1012, FIG. 1 (annotated).

[1.3]

Lee discloses that "integrated push service server 100 receives the push information push_info from the plurality of push application servers 10, 12 and 14 connected through a communication network" ("***the network message server configured to receive, from each of a plurality of network application servers, multiple requests to transmit application data***"). SAMSUNG-1012, ¶[25], FIG. 1; SAMSUNG-1003, ¶[128]. Lee also discloses that push information includes "push_info including a receiving mobile terminal information specifying the mobile terminal that receives the push data, and an associated application ID app_ID

specifying the application for invoking the push data" ("***each such request indicating a corresponding one of the mobile end-user devices and one of a plurality of applications***"). SAMSUNG-1012, ¶[22], FIG. 1; SAMSUNG-1003, ¶[128].

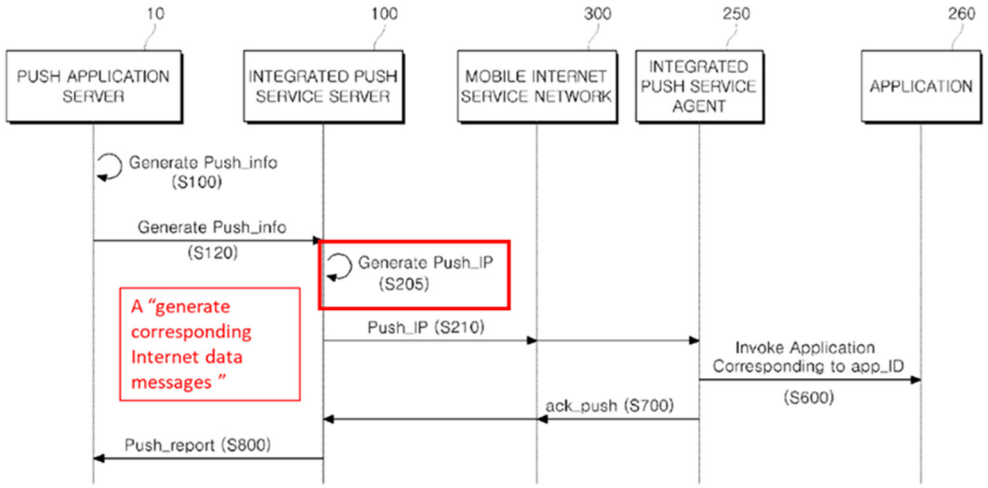


SAMSUNG-1012, FIG. 1 (annotated).

[1.4]

Lee discloses that the integrated push service server 100 "provides the push information push_info to the mobile terminal 200 through an IP push push_IP" ("***the network message server to generate corresponding Internet data messages based on the requests***"). SAMSUNG-1012, ¶¶[25]-[29], [53]-[62], FIGS. 6-7. Indeed, Lee's figures (e.g., FIG. 6 reproduced below) disclose that the integrated

push server 100 "***generate[s]***" the push_IP. SAMSUNG-1012, FIGS. 6-7; SAMSUNG-1003, ¶[129].



SAMSUNG-1012, FIG. 6 (annotated).

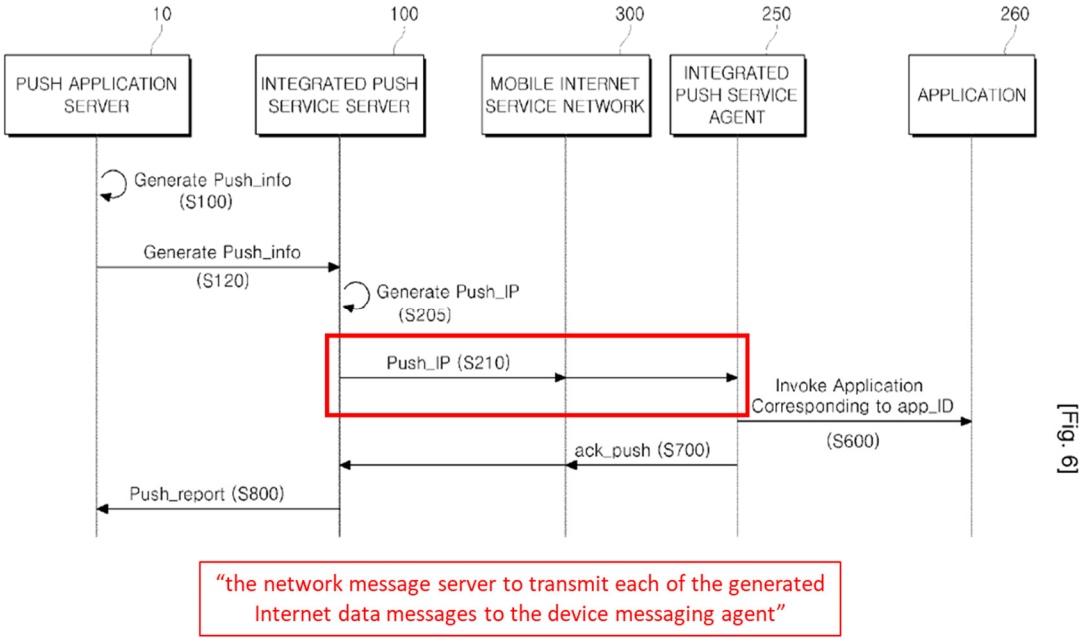
Additionally, Lee discloses that the push_IP "includes at least one application 260 that is to be associated with the push information push_info" and that the push_info "uses [an] associated application ID app_ID … to selectively invoke the application 260" ("***each such message containing at least one application identifier for an indicated application***"). SAMSUNG-1012, ¶¶[25]-[29]. Lee also describes that the mobile terminal 200 "invokes the application 260 compliant to the associated application ID app_ID of the push information push_info to deliver the push data" ("***each such message containing … application data corresponding to one of the requests***"). *Id.*; SAMSUNG-1003, ¶[130].

As Dr. Traynor explains, a POSITA would have also recognized or found

obvious that "***each***" message generated by the network message server would contain an "***application identifier***" and "***application data***" because, without either, the generated message would be meaningless. SAMSUNG-1003, ¶[131] ("a message without an application identifier would leave the device messaging agent with no instructions on where to send the received data, and a message with only an application identifier and no application data would be pointless").

[1.5]

Lee discloses that the "integrated push service server 100 … provides the push information push_info to the mobile terminal 200 through an IP push push_IP" ("***the network message server to transmit each of the generated Internet data messages to the device messaging agent located on the device indicated in the corresponding request***"). SAMSUNG-1012, ¶¶[25]-[29]; SAMSUNG-1003, ¶[132]. Indeed, Lee's figures (e.g., FIG. 6 reproduced below) clearly indicate that push_IP are received by the integrated push service agent 250 ("***the device messaging agent***"). SAMSUNG-1012, FIGS. 6-8. As discussed above, the sending of the push_IP by the integrated push service server 100 would have been performed "***using the corresponding secure Internet data connection for the device indicated in the corresponding request.***" SAMSUNG-1012, ¶¶[13], [24]-[29], FIG. 1; SAMSUNG-1010, pp. 100-103; *see supra* §§III.D.3, III.D.5, [1.2]; SAMSUNG-1003, ¶[132].



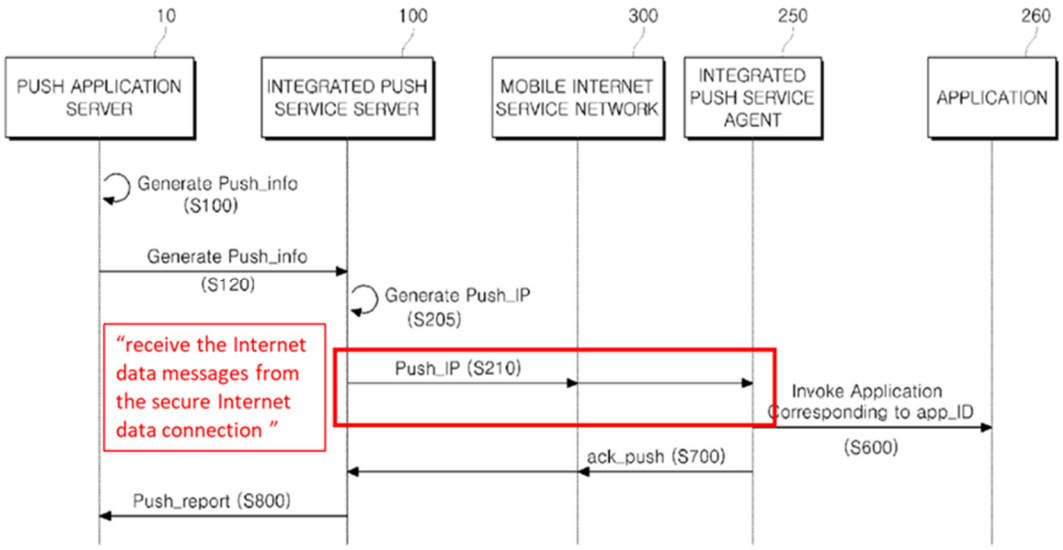
[Fig. 6]

SAMSUNG-1012, FIG. 6 (annotated).

[1.6]

Lee discloses that "the mobile terminal 200 maintains a communication session with the integrated push service server 100 through a CSM (Communication Session Manager) 251 of the integrated push service agent 250" and that "the push information push_info including the push data may be transmitted through the IP push push_IP" (such that the integrated push service agent 250 "***receive[s] the Internet data messages from the secure Internet data connection corresponding to the device executing the device messaging agent***"). SAMSUNG-1012, ¶¶[25]-[29]; SAMSUNG-1003, ¶[133]. Indeed, Lee's figures (e.g., FIG. 6 reproduced below) clearly indicate that push_IP are received by the integrated push service agent 250 ("***the device messaging agent***"). SAMSUNG-1012, FIGS. 6-8; *see supra*

[1.5]; SAMSUNG-1003, ¶[133].



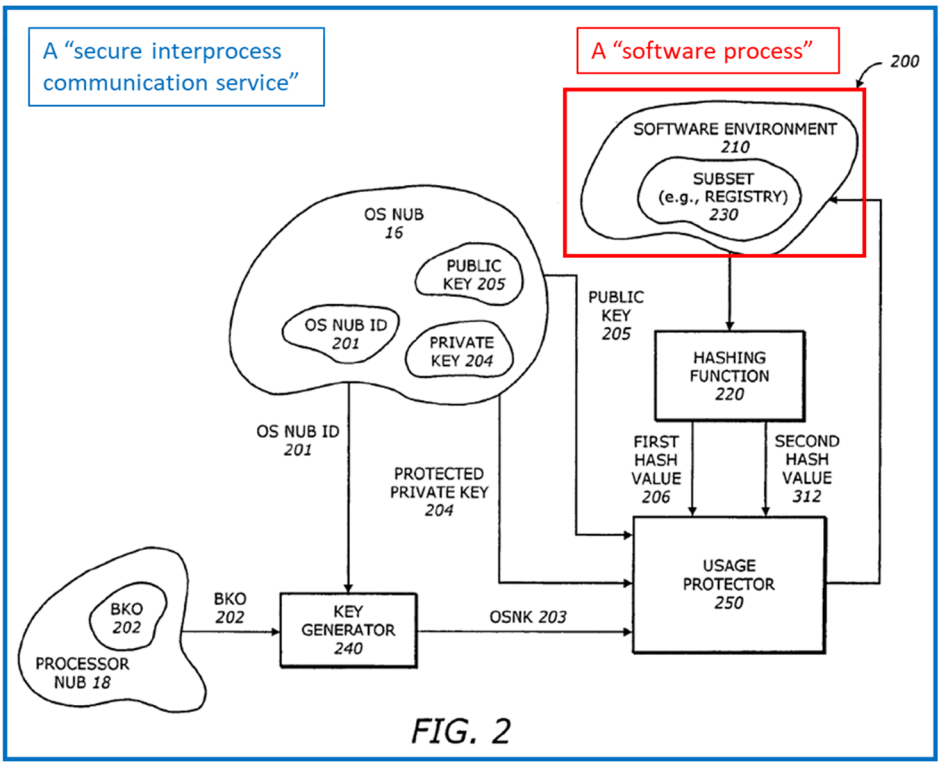
SAMSUNG-1012, FIG. 6 (annotated).

[1.7]

Lee discloses that the push service agent "selectively invokes the application 260 compliant to the associated application ID app_ID of the push information push_info" ("***map the application identifier in the message to a software process corresponding to the application identifier***"). SAMSUNG-1012, ¶¶[28]-[29]; SAMSUNG-1003, ¶¶[134]-[135].

Ellison discloses an "isolated area 70," which is "[a] memory area that is defined by the processor 110 when operating in [an] isolated execution mode." SAMSUNG-1013, 6:1-26, 8:25-32, FIGS. 1A-1C, 2. Ellison refers to this technique, illustrated below in Figure 2, as a "secure platform" ("***a secure interprocess communication service***"). *Id*., 8:25-32, 8:66-67, 9:1-6, 9:28-62, FIG. 2. Ellison

teaches that the secure platform includes a "key generator 240" that "generates a key operating system nub key (OSNK) 203," which is then supplied to "trusted agents." *Id*., 8:66-9:6, FIG. 2. One example of a trusted agent is a "usage protector 250" that "uses the OSNK 203 to protect the usage of [a] subset 230" ("***a software process corresponding to the application identifier***"). *Id*., 9:28-40, FIG. 2. Ellison's usage protector 250 uses a hashing function with the subset 203's ONSK 203 to determine if the subset 203 has been altered following changes (e.g., reads or writes to the subset 203), thereby providing "protection against unauthorized reads, and detection of intrusion, tampering or unauthorized modification." *Id*., 9:47-62; SAMSUNG-1003, ¶¶[135]-[136].



SAMSUNG-1013, FIG. 2 (annotated).

In implementing the Lee-Ellison-Anderson combination, Lee's push service agent 250 would have forwarded push messages to applications, and Ellison's usage protectors would have protected the recipient applications against unauthorized access or modification ("***forward the application data in the message to the software process via a secure interprocess communication service***"). SAMSUNG-1012, ¶[28]-[29]; SAMSUNG-1013, 8:25-32, 8:66-67, 9:1-6, 9:28-62, FIG. 2; SAMSUNG-1003, ¶[137]; *see supra* §III.D.4-5. Accordingly, Ellison's secure platform would have provided protection for applications receiving push messages in Lee's push message system (e.g., malware contained within a push message would be detected using the usage protector 250's hashing function). *Id*.; SAMSUNG-1003, ¶[137].

[3]

Lee describes several different types of applications (e.g., "real time news data for a news application, a chatting message for a peer-to-peer messenger application and an e-mail message for an e-mail application" ("***application data***" for at least a "***first***" and "***second***" application)). SAMSUNG-1012, ¶[22]. As Dr. Traynor explains, a POSITA would have recognized or found obvious that each of these applications would receive application data in different "***format[s]***" because these applications are substantially different in nature (e.g., "real-time news" would be received in a format different than "email"). SAMSUNG-1003, ¶[138].

[4]

As an initial matter, Dr. Traynor explains that this claim "recites only basic encryption/decryption without any additional detail," and as such, a POSITA would have found it obvious for multiple reasons. SAMSUNG-1003, ¶[139].

First, Anderson discloses multiple secure internet protocols that include message encryption, for example, "TLS" and "IPsec." SAMSUNG-1010, pp. 100-103. Indeed, Anderson provides an example TLS protocol exchange where a client and server exchange keys before sending encrypted traffic. *Id*. Once the server and client have authenticated each other, "all traffic is encrypted" ("***the network message server further to encrypt the secure Internet data messages, the device messaging agents further to decrypt each received message***"). *Id*. As Dr. Traynor explains, "[t]hus, multi-layer encryption ('***the network message server further to encrypt the secure Internet data messages***') would have been achievable, for example, through the use of both TLS and IPsec in combination." SAMSUNG-1010, 100-103; SAMSUNG-1003, ¶[140]; *see supra* [1.2], [1.4]-[1.5].

Second, Dr. Traynor explains that it would have been obvious to a POSITA that Lee's integrated push service server 100 ("***network message server***") and integrated push service agent 250 ("***device messaging agent***") would perform encryption/decryption as (1) this would prevent multiple components/applications from

needing to perform encryption as the push server/agent are central to push communication, and (2) it was known in the art that push servers performed such encryption. SAMSUNG-1003, ¶[141]. Indeed, Chou is one example of a push message system that uses a "WAP gateway" (e.g., a network message server) that encrypts content received from a "content server" for transmission to a "mobile client" which then "decodes the response." SAMSUNG-1009, ¶¶[0054]-[0060]. Rakic and Shen provide additional examples of a push server encrypting message traffic. SAMSUNG-1008, ¶¶[0065]-[0068]; SAMSUNG-1025, ¶¶[0056]-[0060], FIG. 5; SAMSUNG-1003, ¶[141].

Dr. Traynor explains that, in each of the above examples, a POSITA would have recognized or found obvious that, in decrypting the messages, the push client would "***obtain the corresponding application identifier and application data***" because this information is included in the encrypted message. SAMSUNG-1003, ¶[142].

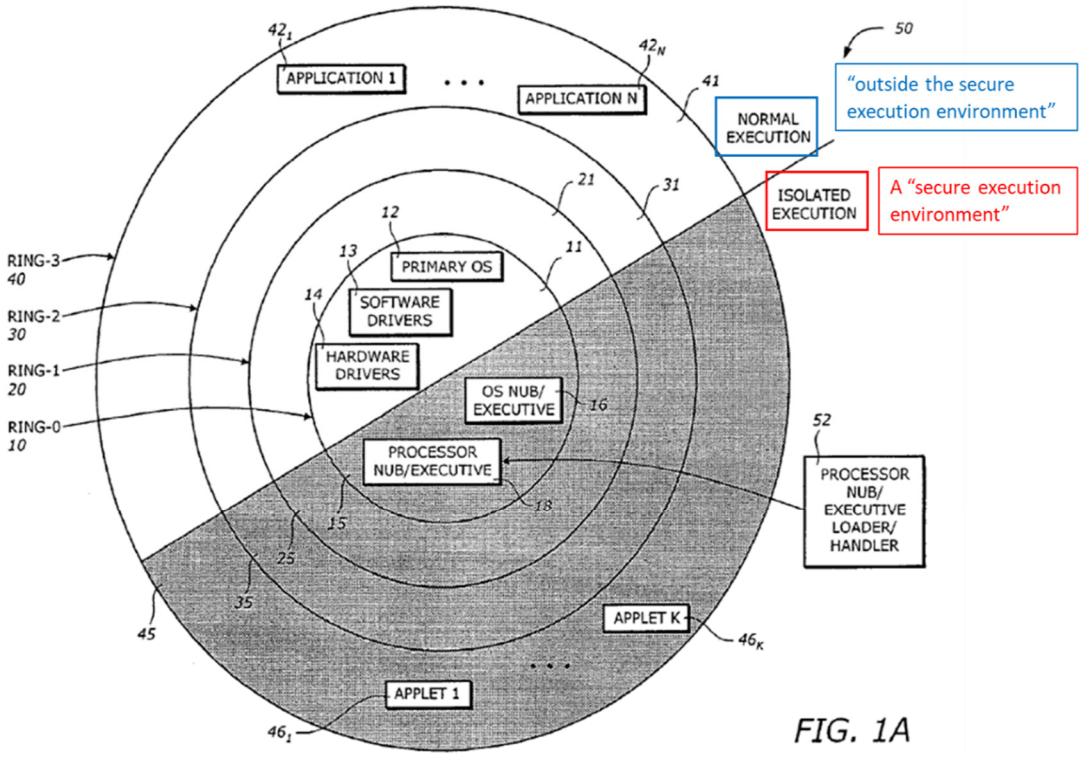
[5]

As Dr. Traynor explains, a POSITA would have recognized or found obvious that "***the secure Internet data messages are transported to the device messaging agent***" using "***one or more of encryption on a transport services stack, [and/or] IP (Internet Protocol) layer encryption***" because these techniques are within the secure protocols described by Anderson. SAMSUNG-1010, pp. 100-

103; *see supra* §III.D.3; SAMSUNG-1003, ¶[143]; *see supra* [1.3], [4]. For example, the IPsec and TLS protocols described above are end-to-end security schemes that can provide "***encryption on a transport services stack***" and "***IP (Internet Protocol) layer encryption***." *Id*. Additionally, Anderson discloses that IPsec is "widely used" by vendors who offer "virtual private network (VPN)" services ("***tunneling***"). SAMSUNG-1010, pp. 100-101; SAMSUNG-1003, ¶[143].

[6]

Ellison discloses both an "isolated execution mode" where "access … is restricted and a "normal execution mode" that "operates in a non-secure environment, or a normal environment without the security features provided by the isolated execution mode." SAMSUNG-1013, 4-65-67, 5:1, 6:1-26, FIGS. 1A, 1C; SAMSUNG-1003, ¶[144]; *see supra* [1.7]. As discussed above, the device messaging agent in the Lee-Ellison-Anderson combination "***executes in a secure execution environment on at least one of the devices***." *See supra* [1.7]. Additionally, the teachings of Ellison allow for "normal" execution, for instance, applications "***outside of the secure execution environment on that device***." SAMSUNG-1013, 4-65-67, 5:1, 6:1-26, FIGS. 1A, 1C; SAMSUNG-1003, ¶[144].



SAMSUNG-1013, FIG. 1A (annotated).

A POSITA would have also recognized and found obvious that certain push_info described in Lee would have required communication from a "***secure execution environment***" to an application or software process "***outside of the secure execution environment***." SAMSUNG-1012, ¶¶[28]-[29], [40], [57]; SAMSUNG-1003, ¶[145].

[9]

As discussed above, the Lee-Ellison-Anderson combination provides network security through a secure internet protocol ("***secure Internet data connection***") and an isolated area ("***secure interprocess communication service***"), which

are "***separately secured***," because each one could provide its security advantages without the need of the other. SAMSUNG-1003, ¶[146]; *see supra* [1.2] and [1.7].

[10]

Lee describes that push_info received from push_IP is received in an "integrated fashion" for "the entirety of applications" (a "***secure Internet data message compris[ing] multiple identifier/data pairs***"). SAMSUNG-1012, ¶[29]. Additionally, Dr. Traynor explains that, because Lee discloses that the integrated push service server 100 can "schedule and transmit the push information push_info," a POSITA would have recognized or found obvious that buffered push_info would be condensed into a single push_IP because this would be the most efficient method of transmitting multiple sets of push_info. SAMSUNG-1003, ¶[147].

[11]

Anderson discloses various secure internet protocols with end-to-end encryption (e.g., the application server to the application), and accordingly, renders this claim obvious ("***the secure interprocess communication service forwards the application data to at least one of the software processes in an encrypted format***" at least because the internet protocol between the server and application itself is encrypted). *See supra* [4]-[5]; SAMSUNG-1003, ¶[149]. Additionally, Ellison discloses various encryption functions performed by the usage protector 250. SAMSUNG-1013, 9:48-13:3. SAMSUNG-1003, ¶[148].

Moreover, as Dr. Traynor explains, end-to-end encryption in messaging applications (e.g., the server to the application) was well known as of the Critical Date. SAMSUNG-1003, ¶[150]. Indeed, CryptoGraf, released in July 2007 for the Symbian and Windows Mobile operating systems, was one such secure messaging application. SAMSUNG-1015; SAMSUNG-1003, ¶[150].

[13]

As described above, Dr. Traynor explains that the secure protocols disclosed by Anderson are "***terminated within the network stack***." *See supra* §III.A.4.[13], §III.D.3; SAMSUNG-1003, ¶[151].

[14]

Anderson discloses that, in secure internet protocols, authentication is performed before data is shared. SAMSUNG-1010, pp. 64-109. For example, Anderson describes a process within the TLS protocol where authentication is performed before sending credit card information to a server. *Id*., pp. 101-102. In this example, a client and a server perform "authentication" via a "key exchange" before "finally … sending the data." *Id*. Anderson describes a similar authentication process for IPsec. *Id*., pp. 100-101; SAMSUNG-1003, ¶[152].

Dr. Traynor further explains that a POSITA would have recognized or found obvious that that authentication would be performed between the "***application***" and "***the network application server corresponding to that application***" before

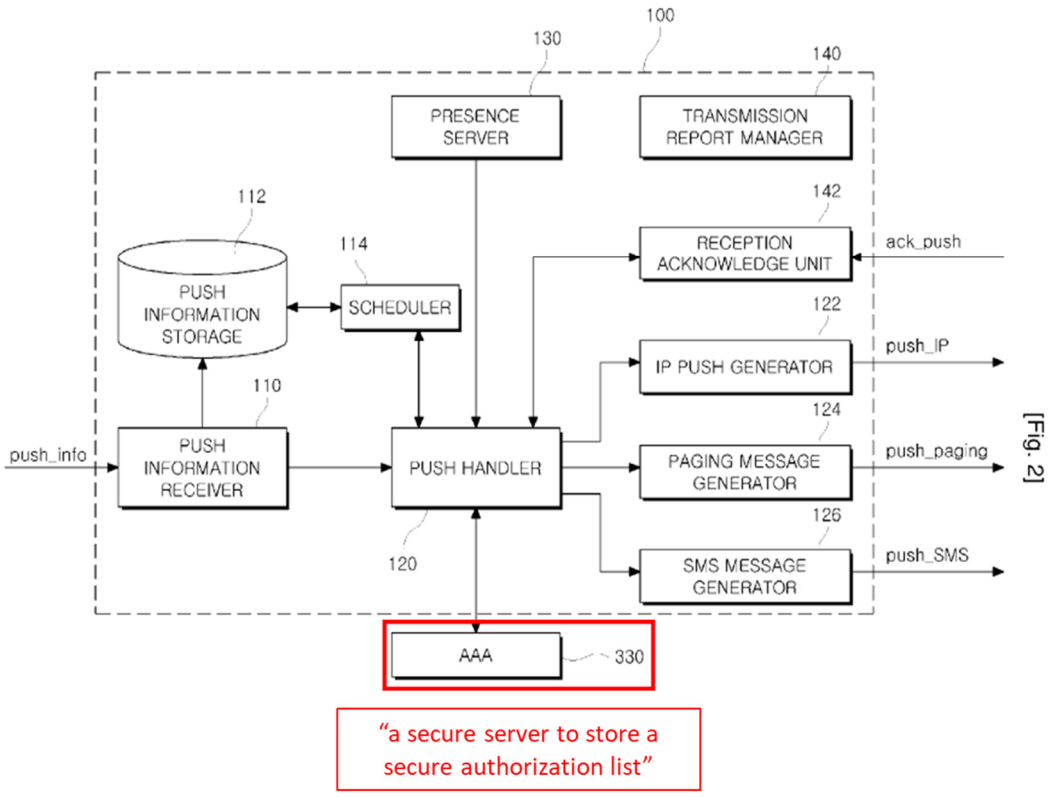
"***passing application data via the device messaging agent on that device and the network message server***" because allowing unauthenticated communication would be a substantial security risk. SAMSUNG-1003, ¶[153]. Indeed, as Dr. Traynor explains, "allowing unauthenticated parties to pass messages in a secure messaging system defeats the entire purpose of securing the messaging system in the first place. Security in a networking system is only as strong as its weakest link (i.e., any and all unauthenticated actors would be a potential security breach)." SAMSUNG-1003, ¶[153].

[15]

As an initial matter, the '117 Patent does not define a "secure server" or "secure authorization list," but discloses "agent level access authorization, which only allows access to the agents that are on the secure authorization list and in which the list is provided by the secure server and signatures are provided by the secure server." SAMSUNG-1001, 42:31-35. While the above disclosure does not recite the features of the claim[10], Petitioner has used these statements to guide the below analysis in the absence of any comprehensive disclosure of the claim features in the '117 Patent. SAMSUNG-1003, ¶[154].

[10] *Supra* note 8.

Lee discloses that the integrated push service server 100 is in communication with a "AAA 330" service (illustrated in FIG. 2 below), which, as Dr. Traynor explains, a POSITA would have recognized and found obvious to be an "Authentication, authorization, and accounting (AAA)" service. SAMSUNG-1012, FIG. SAMSUNG-1003, ¶[155], SAMSUNG-1016; SAMSUNG-1017, Abstract. Dr. Traynor also explains that it was well known in the art that this AAA service would have been established on a "server" ("***a secure server to store a secure authorization list***"). *Id*. Dr Traynor goes on to explain that AAA servers were (and still are) commonly used in the industry by the Critical Date to "control access to computer resources and applications" ("***the secure authorization list indicating the applications and network application servers that are allowed to communicate using the network message server***"). *Id*.



SAMSUNG-1012, FIG. 2 (annotated).

E. [GROUND 2B] – Claims 2 and 16-18 are rendered obvious by Lee, Ellison, Anderson, and Hämäläinen

1. Overview of Hämäläinen

Hämäläinen discloses a method for "facilitating the creation of push messages pertaining to context dependent services and managing their delivery to mobile wireless devices having diverse routing." SAMSUNG-1018, Abstract. Hämäläinen discloses a "content queue" and a "message queue" for "buffering push messages." *Id.*, ¶[0020]; *see also id.*, ¶¶[0008], [0024], [0036], [0053]-[0054], FIGS. 1-2. Hämäläinen also describes a "service profile" associated with the mobile device that can "specify scheduled delivery or delivery triggered by certain

specified events." *Id.*, ¶¶[0007]-[0008]; *see also id.*, [0021]-[0024]; SAMSUNG-1003, ¶[156].

2. Combination of Lee-Ellison-Anderson and Hämäläinen

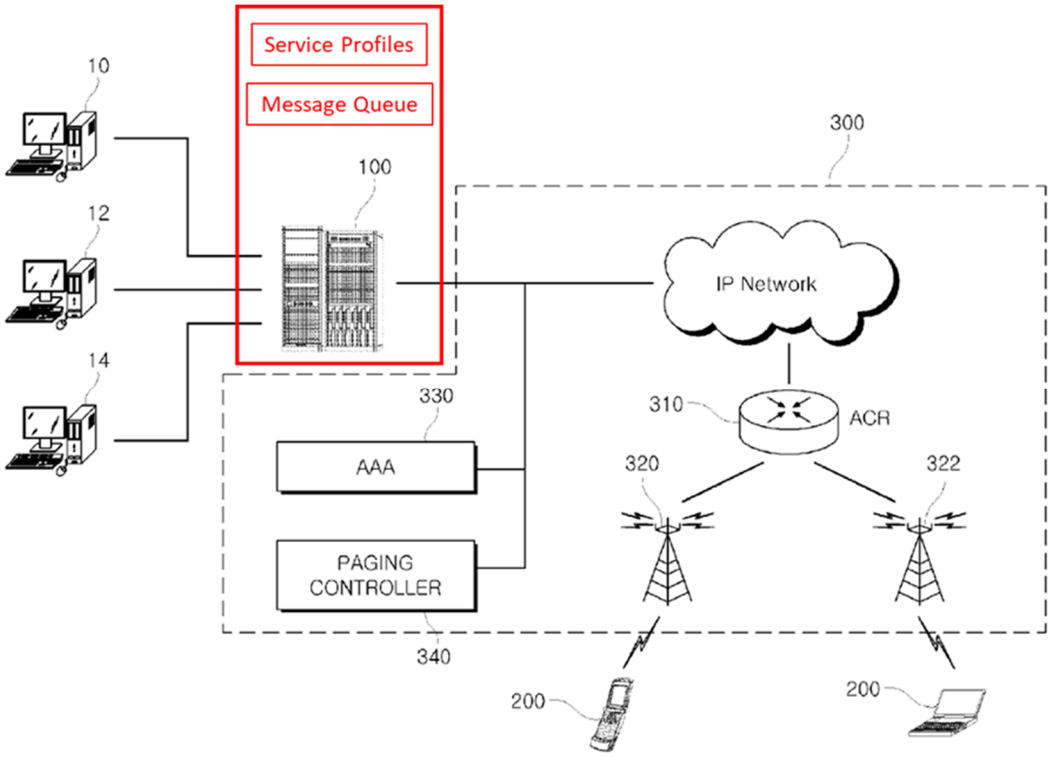
It would have been obvious to a POSITA to combine the teachings of Lee, Ellison, Anderson, and Hämäläinen such that Lee's push message system would collect and buffer messages. SAMSUNG-1003, ¶[157]. As one example, Hämäläinen's teachings of buffering push messages would have been incorporated into the integrated push service server 100 of Lee. SAMSUNG-1012, ¶[34], FIG. 2; SAMSUNG-1018, ¶¶[0008], [0020], [0024], [0036], [0053]-[0054], FIGS. 1-2; SAMSUNG-1003, ¶[157]; *see supra* §§III.D.1-5. As Dr. Traynor explains, a POSITA would have combined Lee, Ellison, Anderson, and Hämäläinen as a POSITA would have naturally searched for implementation details for Lee's push information storage 112. SAMSUNG-1003, ¶[157].

As explained below in more detail, combining Lee, Ellison, Anderson, and Hämäläinen would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results and (2) the use of known technique to improve similar devices (methods, or products) in the same way. *See KSR,* 550 U.S. at 415-421; MPEP §2143; SAMSUNG-1003, ¶[158].

Incorporating Hämäläinen's teachings of buffering push messages into Lee's

integrated push service server 100 would also have been predictable and foreseeable with a reasonable expectation of success because Lee already discloses "schedul[ing]" push message delivery. SAMSUNG-1012, ¶[34], FIG. 2; SAMSUNG-1018, ¶¶[0008], [0020], [0024], [0036], [0053]-[0054], FIGS. 1-2; SAMSUNG-1003, ¶[159]; *see supra* §§III.D.1-5. Additionally, Hämäläinen, like Lee, discloses that its methods can be implemented for "mobile wireless devices" (consistent with the mobile terminals described by Lee). SAMSUNG-1018, ¶[0005]-[0010]; SAMSUNG-1012, ¶[22]-[29]; SAMSUNG-1003, ¶[159].

In an example of the combined Lee-Ellison-Anderson-Hämäläinen system, illustrated below in Lee's Figure 1, Hämäläinen's teachings of buffering push messages would have been incorporated into Lee's integrated push service server 100. SAMSUNG-1012, ¶[34], FIG. 2; SAMSUNG-1018, ¶¶[0008], [0020], [0024], [0036], [0053]-[0054], FIGS. 1-2; SAMSUNG-1003, ¶[160]; *see supra* §§III.D.1-5.

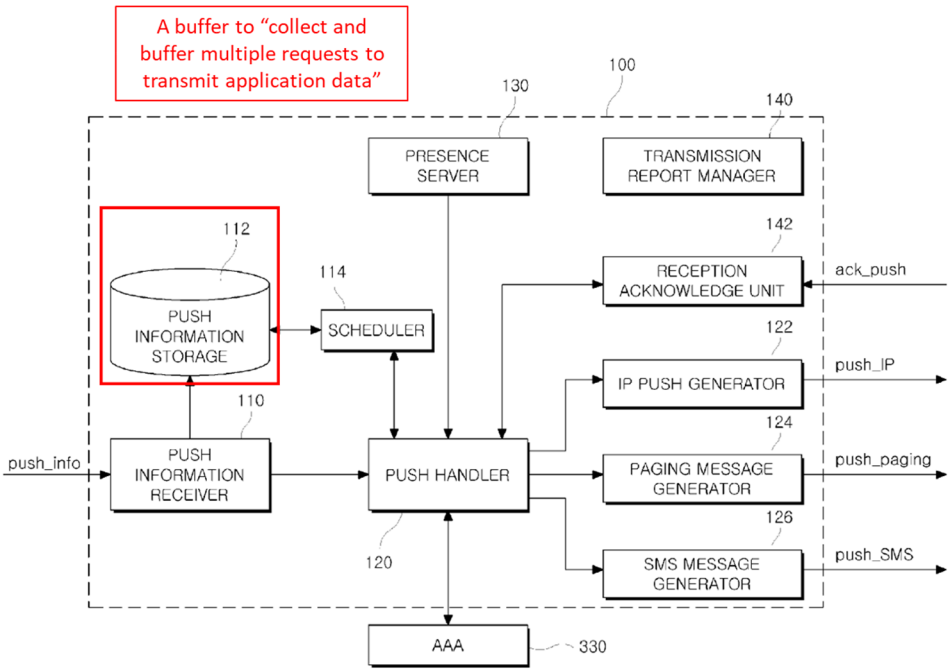


SAMSUNG-1012, FIG. 1 (annotated).

3. Analysis

[2]

Illustrated below, Lee's integrated push service server 100 includes a "push information storage 112" (a "***buffer***"). SAMSUNG-1012, FIG. 2. Lee also discloses that integrated push server 100 can "schedule and transmit the push information push_info or re-transmit the push information push_info by recognizing a communication configuration of the mobile terminal 200" ("***collect and buffer multiple requests to transmit application data to a particular one of the devices***"). SAMSUNG-1012, ¶[34]; SAMSUNG-1003, ¶[161].

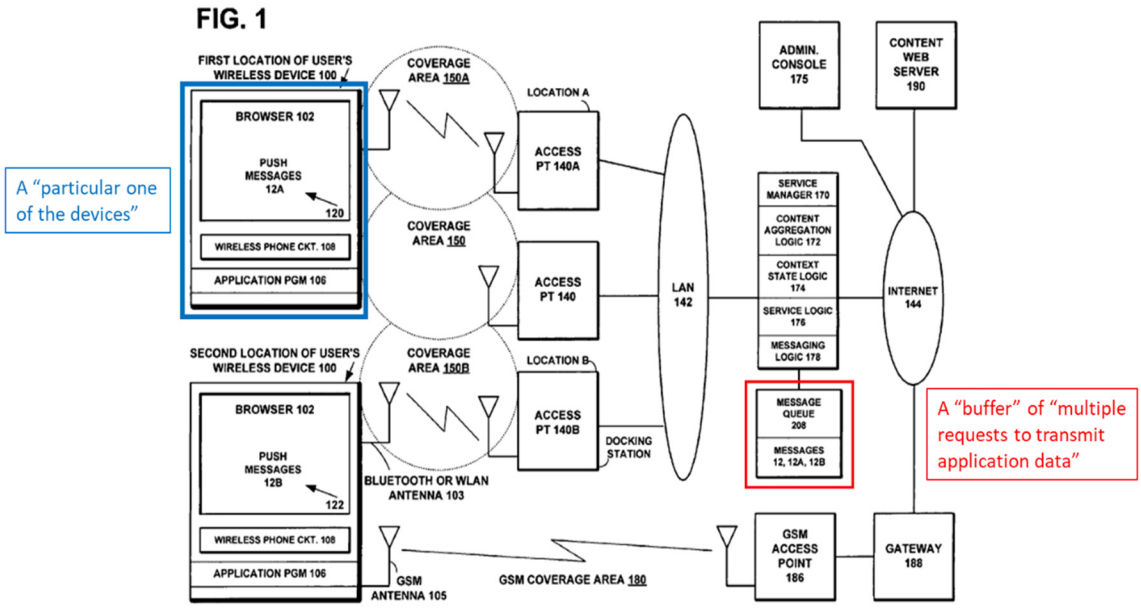


SAMSUNG-1012, FIG. 2 (annotated).

Hämäläinen provides implementation details for Lee's push information storage 112 and discloses a "message queue 208" for "buffering push messages" ("***the network message server further to collect and buffer multiple requests to transmit application data***"). SAMSUNG-1018, ¶[0020]; *see also id.*, ¶¶[0008], [0024], [0036], [0053]-[0054], FIGS. 1-2; *see supra* §III.E.1; SAMSUNG-1003, ¶[162]. Figure 1 below illustrates the teachings of Hämäläinen.

Hämäläinen also discloses that messages are pushed to a mobile device based on a corresponding "service profile" which can "specify scheduled delivery or delivery triggered by certain specified events." SAMSUNG-1018, ¶[0022]; *see also id.*, ¶¶[0007]-[0008], [0021]-[0024]. Because service profiles are unique to

their corresponding mobile device, these profiles specify message delivery (to include de-buffering) for "***a particular one of the devices***." *Id.*; SAMSUNG-1003, ¶[163].



SAMSUNG-1018, FIG. 1 (annotated).

[16]

As discussed above in [2], Hämäläinen discloses that the "service profile" specifies "scheduled delivery or delivery triggered by certain specified events" and includes "characteristics of the contexts that trigger the Service Manager 170 to push messages 12A and 12B to device 100" ("***the network message server transmits the collected and buffered requests to the particular device upon the occurrence of a transmission trigger***"). SAMSUNG-1018, ¶[0022]; *see also id.*, [0007]-[0008], [0021]-[0024]; *see supra* [2], §III.E.1; SAMSUNG-1003, ¶[164].

[17]

Hämäläinen discloses that a trigger event for forwarding a push message can be a "timer event" ("***the transmission trigger is the expiration of a periodic timer***"). SAMSUNG-1018, ¶[0052]; *see also id.*, ¶¶[0034], [0056]; *see supra* [16]; SAMSUNG-1003, ¶[165].

[18]

Lee discloses that the integrated push service server 100 can "schedule and transmit the push information push_info or re-transmit the push information push_info by recognizing a communication configuration of the mobile terminal 200" ("***the transmission trigger is the receipt of a transmission from the device messaging agent of the particular device***"). SAMSUNG-1012, ¶[34]; SAMSUNG-1003, ¶[166].

Hämäläinen also discloses that a "context state change" can be a trigger event. SAMSUNG-1018, ¶[0052]; *see also id.*, ¶¶[0026]-[0033]. One context state according to Hämäläinen is "JOINED," which indicates "the device 100 has joined an access point 140 and is reachable" ("***the receipt of a transmission from the device messaging agent of the particular device***"). SAMSUNG-1018, ¶¶[0026]-[0032]; SAMSUNG-1003, ¶[167].

F. [GROUND 2C] – Claims 7-8 and 12 are rendered obvious by Lee, Ellison, Anderson, and Houghton

1. Combination of Lee-Ellison-Anderson and Houghton

It would have been obvious to a POSITA to combine the teachings of Lee, Ellison, Anderson, and Houghton such that Houghton's techniques of bi-directional push channels and initiating push connections would have been incorporated into the network system of Lee-Ellison-Anderson. SAMSUNG-1005, 23:3-21, 25:4-18, Claim 1, FIG. 8; SAMSUNG-1012, ¶[22]-[29], FIG. 1-2; SAMSUNG-1003, ¶[168]. As Dr. Traynor explains, a POSITA would have combined Lee, Ellison, Anderson, and Houghton to improve the capability of Lee-Ellison-Anderson's network system to respond to push messages and initiate connections with push servers. SAMSUNG-1003, ¶[168].

As explained below in more detail, combining Lee, Ellison, Anderson, and Houghton would have been obvious at least because such a combination would have merely involved (1) combining prior art elements according to known methods to yield predictable results and (2) the use of known technique to improve similar devices (methods, or products) in the same way. *See KSR,* 550 U.S. at 415-421; MPEP §2143; SAMSUNG-1003, ¶[169].

Incorporating Houghton's techniques of bi-directional push channels and initiating push connections into Lee-Ellison-Anderson's network system would also

have been predictable and foreseeable with a reasonable expectation of success because Houghton, like Lee, describes that its techniques can be implemented in "mobile terminals." SAMSUNG-1005, 16:16-36, 17:1-2; SAMSUNG-1012, ¶¶[22]-[29]; SAMSUNG-1003, ¶[170].

2. Analysis

[7]-[8] and [12]

A POSITA would have incorporated the techniques of Houghton's network system into the network system of Lee, as described above in Ground 1A. SAMSUNG-1003, ¶[171]; *see supra* §§III.A.4.[7]-[8], [12], III.F.1.

IV. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. 35 U.S.C. §325(d) – *Advanced Bionics*

Discretionary denial under the Board's §325(d) *Advanced Bionics* analysis is not warranted. *See Advanced Bionics, LLC v. Med-El Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, 8-9 (PTAB Feb. 13, 2020) (precedential) ("*Advanced Bionics"*).

During prosecution, the '117 Patent was allowed on the first action without any rejections. SAMSUNG-1002, pp. 34-37. Accordingly, none of the prior art references advanced in this Petition were previously before the Office. *See generally*, SAMSUNG-1002. Moreover, the same or substantially the same arguments were not previously presented to the Office. *Id*.

Accordingly, the Office did not consider any one of Houghton, Kalibjian, Munson, Rakic, Lee, Ellison, Hämäläinen, or Anderson. *Id*. Moreover, Petitioner has shown a reasonable likelihood that it would prevail that at least one of the Challenged Claims is unpatentable over the applied art based on the current record. *Supra* §IIIA-F; *see Tokyo Ohka Kogyo Co., Ltd. v. Fujifilm Elec. Materials U.S.A., Inc.*, PGR2022-00010, Paper 9, 8-9 (PTAB June 6, 2022). Therefore, Petitioner has demonstrated material error by the Office, and discretionary denial is not warranted.

B. §314(a) Denial is Not Warranted

The merits of Petitioner's arguments are compelling, and the evidence in support is substantial. That "alone demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*." SAMSUNG-1020, 4-5. Moreover, the *Fintiv* factors do not favor denial.

Factor 1 is neutral because neither party has requested a stay in co-pending litigation.

Factor 2 is neutral because the Court's trial date is speculative at this point and subject to change. The Board will likely issue its Final Written Decision around May/June 2025, approximately 4-5 months after the currently scheduled trial date (January 6, 2025). SAMSUNG-1021, 2. However, as the Board and Director have previously recognized, "scheduled trial dates are unreliable and often

change." SAMSUNG-1020, 8.

Factor 3 favors institution because Petitioner has diligently filed this Petition months ahead of the one-year time bar, while the EDTX Litigation is still in its early stages. Beyond exchanging preliminary infringement contentions, the parties and the District Court have yet to expend significant resources on invalidity. SAMSUNG-1021. Moreover, by the anticipated institution decision deadline in May/June 2024, the EDTX litigation will still be in early stages—both fact and expert discovery will be ongoing, and the *Markman* hearing will not have yet occurred. *Id.*

Factor 4 also favors institution because Petitioner has provided a stipulation that it will not pursue the IPR grounds in the district court litigation. SAMSUNG-1023. Thus, "[i]nstituting trial here serves overall system efficiency and integrity goals by not duplicating efforts and by resolving materially different patentability issues." *Apple, Inc. v. SEVEN Networks, LLC*, IPR2020-00156, Paper 10, 19 (June 15, 2020); *see also Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019,-01393, Paper 24, 12 (June 16, 2020); *Google LLC v. Flypsi, Inc.*, IPR2023-00360, Paper 9, 36-39 (August 2, 2023).

Factor 5: The parties in the parallel EDTX litigation are the same.

Factor 6 favors institution because the merits of this Petition are compelling, as described in this Petition.

V. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Please charge fees to Deposit Account 06-1050.

VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Samsung") are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '117 Patent is the subject of a civil action, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:23-cv-00103, E.D. Tex., March 10, 2023 (SAMSUNG-1004). Petitioner and Headwater are also involved in case nos. 2:22-cv-00422 and 2:22-cv-00467, also in E.D. Tex.

Petitioner is not aware of any other disclaimers, reexamination certificates, or IPR petitions addressing the '117 Patent.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email:IPR39843-0165IP1@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Jennifer Huang, Reg. No. 64,297 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above. Petitioner consents to electronic service by email at IPR39843-0165IP1@fr.com (referencing No. 39843-0165IP1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, jjm@fr.com, and jjh@fr.com).

Respectfully submitted,

Dated November 17, 2023

/Jennifer J. Huang/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Jennifer Huang, Reg. No. 64,297
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2024-00003)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,904 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated November 17, 2023

/Jennifer J. Huang/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Jennifer J. Huang, Reg. No. 64,297
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on November 17, 2023, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667